# Interview – Lev Topor

https://www.e-ir.info/2020/09/28/interview-lev-topor/

E-INTERNATIONAL RELATIONS, SEP 28 2020

**This interview is part of a series of interviews with academics and practitioners at an early stage of their career. The interviews discuss current research and projects, as well as advice for other early career scholars.**

Lev Topor is currently a senior research fellow at the Center for Cyber Law and Policy at the Haifa University. His research interests are online extremism, racism, terrorism, fraud, anonymous communications, cyber warfare and international affairs. Topor's work is interdisciplinary but grounded in the field of political science and international relations. He completed his Doctorate at the Bar Ilan University in Israel and his dissertation examined anti-Semitic and anti-Zionist trends in the British Labour Party under the rule of Jeremy Corbyn MP, specifically between 2010 and 2018.

**What (or who) prompted the most significant shifts in your thinking or encouraged you to pursue your area of research?**

My two main fields of research are different from one another – one is antisemitism studies (and racism in general) and the other is cyber and politics. My early motivations to research each field were also quite different, however, I quickly discovered that these two fields are deeply connected together nowadays in the information age. In the beginning of my academic education, I did not think I would be engaged in academic research but rather in policy-oriented work. When I enrolled to pursue my Master's degree in diplomacy studies in the Tel Aviv university, the curriculum focused on diplomacy, negotiations and international affairs. Further, during the writing process of my Master's thesis (supervised by Dr. Udi Sommer), which dealt with the Israeli-Palestinian peace process, I became aware that nationalists, on both sides, prevent the voice of the moderate public to be executed. I also became aware that many countries worldwide promote antisemitism and anti-Zionism to undermine Israeli negotiations and global legitimacy. Following this research, I decided to examine the case of antisemitism in the British Labour Party between 2010 and 2018. This topic is extremely interesting and elusive since leftists are seldomly perceived as racists. Yet, some radical leftists are engaged in antisemitism, even though they claim that it is merely a side effect of their anti-Zionist perspectives.

Just before I received my PhD in late 2019, my PhD advisor, Prof. Jonathan Rynhold, encouraged me to deepen my understanding of the issue by examining other spheres and domains. Since I had cyber-related experience from outside academia, I decided to explore antisemitism and racism on the right side of politics as well. This also led me to look into the racist scene on the dark web, where web users generally feel anonymous and protected to publish their real opinions – uncensored and non-politically correct. During this time period, I published an article in the Journal of Contemporary Antisemitism about antisemitism and racism in the dark web and it won the prestigious Annual Robert Wistrich Award from the Vidal Sassoon Center for the Study of Antisemitism in the Hebrew University of Jerusalem. Prof. Rynhold and the PhD advisor in our department, Prof. Jonathan Fox, encouraged me to pursue another research topic – cyber and politics, in order to be a more diverse scholar and appeal to a larger portion of academia. This summer I finished a year of Post-Doctoral studies at the Center for Cyber Law and Policy at the University of Haifa, with which I am now affiliated as a Senior Research Fellow.

**You frequently discuss anti-Semitism in relation to your other research interests, including cyber**

**influence and the dark web. Why is it important to focus on such intersections and what have they highlighted?**

The cyber domain is currently the largest and most powerful agent of globalization. Facts, ideas and opinions are traveling faster than ever between countries and communities. This is extremely positive as it helps humankind stride forward. Yet, some international actors, mainly states or extreme organizations, utilize the cyber domain for their own strategic goals. For instance, they spread mis/disinformation, fake news, to pursue their goals and undermine their adversaries. Global powers spread mis/disinformation about the current Coronavirus crisis to gain relative power while they undermine their adversaries. In another example, white supremacists blame Asians, Blacks, Jews, Muslims and others with the outbreak of the pandemic as if it was a sinister plot to undermine the white race.

Racism is very prominent on social media and around the web in general. Its siblings, mainly extremism, terrorism and discrimination are also very prominent on the web nowadays. Even global adversaries utilize the cyber domain and racist ideologies to sow panic and chaos in the domestic arenas of their enemies. Thus, racism is a real and dangerous tactic of cyber warfare – of cyber influence campaigns. For instance, some global adversaries of the Western world are constantly spreading fake news on social media about immigration – the Brexit issue or the past couple of Presidential elections in the US are very significant examples in that regard. The disturbing fact is that these trends are a part of the global competition for influence, power and hegemony and racism is simply a tool or a side effect.

Many might disregard cyber bots and trolls and suggest these should simply be ignored and that it does not really matter who is behind them – intelligence agents of another country or right-wing racists. However, reality is complex, and these two groups promote one another. The cyber domain is complex in the sense that even simple and ungrounded facts can quickly spread worldwide and reach millions of internet users. This means that with a few mouse clicks, perception and ideas can be manipulated.

Moreover, specifically in regard to the dark web and to other anonymous forms of communication, many racists might be socially discouraged to be openly racist. Some might even be afraid or ashamed to engage with a nationalist or racist group in their private and spare time outside their usual social spheres. The dark web enables them to promote and develop their extreme ideas and communities without fear of social judgment, monitoring or legal prosecution (as some countries forbid online racism by law). Thus, the moderate voice, as a global society, does not eradicate racism. We simply turn a blind eye on this issue since it is not very prominent, but it does exist and grow. This also serves politicians as they sometimes base their ideas on fake news or ungrounded information from unreliable sources from the dark web or from secure Telegram groups (and other anonymous platforms).

**Your most recent publication explored why global powers spread conspiracies amid the pandemic. How is cyberspace shaping this "global battle of narratives?"**

In my short article for the Journal of International Affairs, I exemplified and argued that global powers are spreading conspiracies since they do not wish to waste a 'good crisis' and since they perceive the situation as one in which they can gain power and strengthen their global position while also undermining their adversaries by blaming and defaming them. Interestingly, the actual place of the outbreak is the only undisputed fact nowadays. The origin, medical information and other related conspiracies are all debatable now as most countries tried to distance themselves from blame and associate the virus with others. For instance, the US (and other countries) blamed China for hiding the severity of the issue in the very beginning of the outbreak. Following this, China began spreading the idea that the US Army was the one who brought the virus to China in the first place. Less powerful countries like Iran or Turkey began spreading anti-Semitic conspiracies arguing that the Jews and Israel developed and spread the virus to gain more control in the Middle East – this, of course, is part of their general anti-Israeli campaigns. I discussed the issue of antisemitism and the Coronavirus in another short article in Fathom Journal.

I've already explained how the cyber domain acts as a perfect marketing tool to spread ideas and information. This is also true when discussing the Coronavirus pandemic and attempts by countries to shape the narrative of the pandemic in a way that can benefit them and undermine their global adversaries. If we compare current global

politics to the era of the Cold War, it can be argued that each side, the American and the Soviet, did not influence much inside the domestic arena of the other, even in times of crisis. In contrast, nowadays, cyberspace allows users worldwide to develop and promote their own narratives and perspectives on issues and official information is no longer perceived as credible as is once was. If the Soviet Union had an 'Iron Curtain' to protect it, while the US had its self-regulatory systems to protect itself as well, then now cyberspace is so widespread that it is very difficult to regulate and monitor online content, especially on secure and anonymous platforms. Interestingly, as my co-author and I have recently argued, Russia and China have a more protective cyber domain compared to the US or the EU.

You, me, and every other social media user know that arguing on Facebook or Twitter threads is extremely discouraging and a good bot or troll will win debates on many occasions by exhausting moderate users. Now, it is also important to understand what, or who, an internet user really is. Many internet users can be compared to the moderate voice in politics, these are you, me, and generally people of moderate opinions which are not grounded in any extreme ideology and, while on social media, do not seek to engage in conflict with others. Yet, some internet and social media users have sinister plans. Some, like Jihadi extremists, seek to promote antisemitism, anti-Zionism and anti-Western ideas in general. Others, like white supremacists and neo-Nazis, seek to blame all of their social and domestic problems and failures on immigration, on Blacks, on Jews, on Muslims, and so on. Another type is the state-operated or state proxy internet users which promotes, knowingly and purposely, mis/disinformation to present their own country in a positive light while presenting other competing countries in a negative light. As I have mentioned, global actors like China, Russia, Iran, Turkey and even the US are in a constant struggle to shape the narrative of others – in this case, they aim to shape the blame for the pandemic. Their basic concept is this – if [state] 'A' can blame [state] 'B' with the outbreak and convince 'B's domestic arena of mismanagement, it can lead to domestic chaos which will undermine 'B'. In turn, it also means that 'A' can gain power and influence over 'B'. Following this, any third party, for example 'C', can also be convinced to side with 'A' instead of 'B'. In this case of no accepted facts, two are stronger than one. Thus, just imagine what China could have caused if its conspiracy of the US Army bringing the virus to China would have convinced America's allies. If we compare this situation to the Cold War, again, it means that China might bring countries closer to it and push the US from the global premier.

**Given the upcoming US presidential elections and escalating Chinese provocations in disputed territories, what cyber interventions can we expect? Who are the likely key players?**

During election times (but not only), the US is like a pie – everybody wants a piece. That is, every country that depends on American decisions, and there are quite a few, seeks to influence American domestic politics in order to benefit from a leader who is more likely to act positively with it. China and Russia are the obvious key players. The most frequent cyber operations that took and take place are influence operations that promote and market a candidate over another alongside their key values. Since there is no binding international law concerning mis/disinformation or even cyber espionage, and since cyber forensics and attack tracing is extremely complicated, international actors can safely promote their own mis/disinformation campaigns with no fear of retaliation. Thus, I suggest that the cyber interventions we will likely see in the near future are mainly 'fake news' and espionage. Here, I can only present a very general and incomplete outline to answer this question.

As for Americas' adversaries, they are promoting online information on fake news websites and on social media. They even leak certain information to the dark web or to anonymous messaging applications. China and the US are competing for influence and a grip in the South China Sea. This, alongside their ongoing "trade war" and their attempts to influence Hong Kong, Taiwan or North Korea-related issues. China is also biting into Western territory of influence in other parts of the world like in Africa or the Middle East. This situation means that China is likely to promote an American leader whom it perceives will not rush to engage in conflict but rather in dialogue and negotiations.

Russia is another global competitor of the US (and of China) and it mainly competes for influence and a grip in Eastern Europe, mainly to undermine NATO. After many years of Western influence in countries like Ukraine, it is obvious that Russia will act to protect its Western backyard. Russia is also competing with the US over influence in the Middle East and in other parts of the world. Yet, I suggest that its main area of influence was, and still is, Europe, simply because of the cultural bond with the US. This means that Russia is likely to promote an American leader that

will weaken the strong US-EU bond by being less accepted by his European counterparts. Other international players are North Korea and Iran which seek to ease Western pressure and sanctions over them.

Interestingly, key US allies like Britain, Germany, France, Israel and others are also promoting certain online content in an attempt to promote their own favorite candidate, however, they are doing so openly. These types of online influence campaigns generally promote positive values and are generally not misinformative. In contrast to state-sponsored propaganda in the cases of China or Russia, the ones who promote online content in Western countries are mainly organizations and the civil society. Moreover, while America's adversaries promote negative aspects of their least favorite candidate alongside their promotion of the favorite candidate, America's allies are likely to promote mainly positive aspects of their most favorite candidate.

**How is the COVID-19 pandemic shifting countries' cybersecurity priorities?**

As described previously, global adversaries 'jumped' on the opportunity to benefit from a global crisis. Since international law is lacking, mis/disinformation is constantly spreading online, turning the pandemic into an 'infodemic' of fake news. This infodemic is not just about finding a scapegoat, it is also about actual public health and safety. That is, some online users suggested that the virus is fake and social distancing or quarantines are not needed, that these are only a way for the authorities to control populations. This type of misinformation can lead to a rise in death tolls and it is very worrisome. Additionally, with the race to find a vaccine, it was also reported that countries tried to spy on each other and steal vaccine formulas.

I foresee that many countries will prioritize their online safety and security over freedom of speech and access to information. This can be a very slippery slope in terms of state monitoring, surveillance, and people's right to privacy. Yet, restrictions, more regulation and monitoring might now be implemented by countries that seek to resist foreign influence as the COVID-19 case exemplified open and under-regulated cyber domains are more likely to be attacked. The Chinese and Russian cyber domains are very regulated, I assume that European countries and the US will push for more regulations in their respective cyber domains in the future, at least against external flow of information.

**What are you currently working on?**

I am currently working on several research projects in my two major fields of research as well as another project that combines the two. In the field of antisemitism and racism, I am working on projects that analyze and compare racism on the right and on the left. Interestingly, the right-wingers and the radical left-wingers have different explanations for their racism, and even different types of racism in general. Yet, these two spheres do have some similarities which I plan to analyze and explore.

In the field of cyber warfare and cyber politics, I am working on theories and approaches towards cyber influence campaigns and on the cyber domain in international relations perspectives. I also work on anonymous communication and cyber socialization. The combined project seeks to study online racist communities.

**What is the most important advice you could give to young scholars?**

I am a very young scholar myself now – graduated in late 2019 with a PhD from the department of political science. After a year of Post-Doctoral studies, most of which I have spent outside the University by myself due to the global pandemic, and after publishing several scholarly articles and completing a book manuscript, I can advise younger scholars which are now in grad-school to try and be more interdisciplinary. This can be done by developing another set of skills, knowledge or by collaborating with others. If one has experience from outside academia, he or she can try and turn this experience into research and publications. Another important piece of advice I can suggest is to have an agenda – do not be afraid to openly state your agenda and even connect your research to policy-oriented goals, even if some peers or even senior scholars might disagree. In my opinion, scholarly work is useless unless it has a positive social effect, unless it actually promotes something good.