COUNCIL on FOREIGN RELATIONS

Center for Preventive Action

1777 F Street, NW, Washington, DC 20006
tel 202.509.8400 fax 202.509.8490 www.cfr.org

Conflict in a Connected World Roundtable Series Summary
Washington, DC
July 28, 2013

This roundtable series was made possible by Google Ideas and the Council on Foreign Relations' (CFR) Center for Preventive Action.

Summary: Contemporary conflict is being increasingly shaped by information technology. The internet has become a vital new battleground while social media and other mass communication tools now comprise a valuable virtual arsenal for waging war—not only for the immediate combatants but also for interested parties beyond conflict zones. The importance of these technologies to the outcome of political contests and violent conflicts is only likely to grow in the future. As a consequence, the traditional separation of combatants and non-combatants as well as parties and non-parties to a conflict based on physical proximity or declared association is becoming progressively blurred and even meaningless.

Over the course of two months, the Council on Foreign Relations (CFR), in partnership with Google Ideas, convened a series of roundtables to explore the growing importance of information technology to political contest and violent conflict. Because of the extraordinarily broad nature of the subject, the series concentrated on two core themes: first, how technology has changed the nature of political repression, and second, how technology has changed our understanding of traditional conflict. The series brought together a diverse range of experts, from engineers to senior U.S. policymakers to activists from Iran, Syria, and Tibet, among other countries. While numerous specific observations emerged from the discussion, some general insights seemed significant. First, certain states are engaged in a deep campaign of "digital repression," and changes to U.S. sanctions policy may make it harder for such states to censor, monitor, and harass their own citizens. Second, information technologies have profoundly changed how we understand conflicts, and so individuals who affect policy have a responsibility to understand these tools. This roundtable series is just the first attempt to help policymakers in this process of understanding.

* * *

For people living in countries like Iran, Syria, and China, online conflict is an everyday part of their lives. From censorship of political content, to surveillance of Internet activity, to occasional reprisals and harassment both on the Internet and off, what we might call "digital repression" is well

understood by the citizens and activists who live under authoritarian governments. As the series revealed, not all the tools of digital repression are technical and those that are not always well understood, even by activists who work hard to protect themselves on the Internet. As examples across many countries demonstrated, online repression by both state and non-state actors is becoming increasingly complex, and increasingly intertwined with broader campaigns of offline repression.

Today's Internet censors—and there is none as prominent or powerful as the Chinese government—employ a variety of tools to prevent users from receiving the content they seek. While sophisticated software for identifying and blocking material exist, governments increasingly rely on legal mechanisms to keep forbidden content off the Web. By imposing intermediary liability restrictions on local Internet companies, countries like China put the onus of censorship on third parties who must take pains to block their users from creating any potentially offensive material.

Surveillance is also becoming increasingly complex and indirect. Countries like Iran use deep packet inspection (DPI) to monitor Internet traffic within its borders. In response, citizens have begun using so-called virtual private networks (VPNs) to encrypt Internet traffic. Yet troublingly, repressive regimes have begun selling faulty VPNs to download malware onto users' machines. In this way, digital repressors are monitoring their citizens with the very tools citizens use to avoid surveillance.

Finally, reprisals can take a variety of forms, and are perpetrated by both state and non-state actors. A common tactic of digital reprisal is the so-called distributed denial of service (DDoS). In such attacks, malicious groups gain control of "zombie" computers, which they use to overwhelm enemy websites with traffic, temporarily shutting them down. The Syrian government has taken down activist sites using this tactic. But non-state actors can employ DDoS attacks as well: groups like Anonymous are well known for shutting down the sites of major companies like Sony and Mastercard. The tactics of digital repression, it appears, are not limited to governments alone.

In few countries do online and offline repression intersect more directly than in Syria today. Since before the civil war began, the so-called Syrian Electronic Army (SEA)—a misnomer, since it is not actually a part of the Syrian army—has used a variety of tactics to bully, intimidate, and impede activists on the ground. It has used complex DPI technology to view unencrypted Internet traffic and monitor users' behavior in real time. It has issued reprisals by creating fake Facebook and Skype pages to steal passwords, and then torturing users with the information they gain. In moments of crisis, it has literally shut down the Internet in the country. Yet not all its actions are so heavy-handed: the SEA has compromised users' privacy in more subtle ways as well. For instance, it has throttled the encrypted version of Facebook, though has not blocked it. The noticeably slower performance has driven users to the unencrypted version of the site, which the SEA can monitor easily. The sense one gets from these actions is that digital repression is in every way an important and integral part of the Syrian government's larger campaign of offline abuse.

There are a number of steps foreign governments could take to help address these attacks. If the United States is reluctant to engage in a direct conflict in Syria, it can provide long-range WiFi over which activists and rebels can communicate. It can also help to distribute bespoke programs like Tor

and Psiphon, which have been developed specifically to help users bypass firewalls and escape surveillance. Finally, it can share updates for common software programs like Windows and Internet Explorer, older versions of which leave vulnerabilities for citizens and activists. Repressive governments exploit these vulnerabilities to install malware on users' machines. In fact, the Syrian government used a hole in an older version of iTunes to do exactly that. Simply by upgrading to the latest versions of desktop software, users may dramatically improve their security and protect themselves from repressive governments.

In theory, citizens in repressive states should be able to download easily anti-circumvention tools and software patches. Yet in practice, citizens are severely restricted from access to either. Sometimes these restrictions are imposed by repressive governments, but sometimes they are imposed as part of a sanctions regime. Until recently YouTube and Google Chrome were blocked in Iran: YouTube was blocked by the Iranian government, but Chrome was blocked by the U.S. government.

It seems clear that sanctions policy should exclude at least some of these important technologies. Sanctions on information technologies have little real impact on the government, but greatly affect everyday users. While existing sanctions have made it difficult for government elites to obtain restricted technology, such elites possess far greater capacity to circumvent foreign-imposed restrictions than do average citizens. Further, sanctions put everyday users in danger. By preventing activists from obtaining counter-censorship software, or from updating this software, some sanctions may increase the risk of activists working to affect change in these countries.

The U.S. government is beginning to recognize this. For one country—Iran—sanctions policy has evolved over several years to reflect activists' real need for anti-circumvention tools and proper software updates. In September 2010, the United States began allowing tech companies to apply for licenses to export their tools to Iran. Certain free services like Microsoft Messenger were initially permitted into the country, and then a handful of for-pay services followed. Finally, one week before a "Conflict in a Connected World" roundtable on the subject, the U.S. Department of the Treasury issued a general license for certain technologies to be exported into the country without a petition. Now Web browsers, email clients, and blogging tools can all be exported to Iran without going through an application process. These new exemptions reflect an evolving understanding within the U.S. government of the importance of IT as part of broader sanctions strategy.

As part of this process, the U.S. government has had to make important decisions about which technologies are primarily benign, and which are primarily harmful. For instance, the government determined that tools like keystroke logging software have legitimate uses, but would primarily be used for repressive purposes. Similarly, Web browsers can also be used for either good or ill, but seem to have more positive than malign uses. Assessments such as these can be difficult, and even overwhelmingly positive technologies can be enormously destructive in the wrong hands. The reputational risk of such technologies being misused is real. As governments wrestle with these important challenges, they should turn to experts on these technologies to assist with the evaluation. While there is a risk associated with any change in sanctions policy, there is a similar risk of making no change, one which policymakers should recognize.

Regardless of any changes to future sanctions regimes, the importance of social media in the conflict is already enormous. In particular, the Syrian civil war has been understood by foreigners almost exclusively through the lens of social media. With limited ability for journalists to enter the country, the world has watched the evolution of the conflict on sites like Facebook and YouTube, where literally hundreds of thousands of amateur videos have been uploaded since the war began.

Ironically, this information is not accessible to people working in many American intelligence agencies, so much of U.S. understanding comes from analysis produced at think tanks. Participants from these organizations gave specific examples of how they were using online video to gain insights from the Syrian conflict. For instance, by tracking the mention of rebel group names on social media, one analyst was able to graph the evolution of the opposition movement, the growth of certain armed factions, and the decline of others. Another analyst, working with an on-the-ground reporter, was able to use YouTube videos to identify shipments of arms traveling through Croatia to Syrian rebels.

At times, insights from these conflicts emerged from just a few frames of online video. Extracting insights from these bits of data requires detailed analysis and deep understanding of the issues involved. In other words, little of this work can be automated. Given the explosive growth of social media content coming from the conflict, the challenge of gaining insight from social media content is only becoming harder. In a sense, the Syrian civil war is just the beginning: future wars will be even better documented and the relevance of social media and associated challenges are likely only to grow.

Recognizing these trends, participants involved in the analysis of social media agreed that they needed better tools for sharing, commenting on, and synthesizing insights about social media in Syria. Existing software is simply too expensive, or in some cases, too complex for analysts to use. Participants sought simple ways to coordinate their analyses, and there may be an opportunity for technology companies to assist in this effort.

* * *

Technology is changing the nature of conflict: both how people engage in it, and how they understand it. While technology can be part of the solution to "digital repression," policy must play a role here as well. By carving out licenses for certain technologies, the U.S. government can protect civilians while empowering activists to pressure their own governments. The U.S. government should consult experts on these tools, either from the private sector or from those working independently, to evaluate which technologies to include or exclude from sanctions regime.

It is clear that social media is having a dramatic impact on our understanding of current conflicts, and that the importance of this new source of intelligence will only grow over time. The challenge now is to find a way to deal with the wealth of data available to analysts. New tools must be developed to help analysts deal with this data. In turn, policymakers who must react to analysts' findings have a responsibility to understand these technologies themselves. This roundtable series is just a first step towards that understanding.