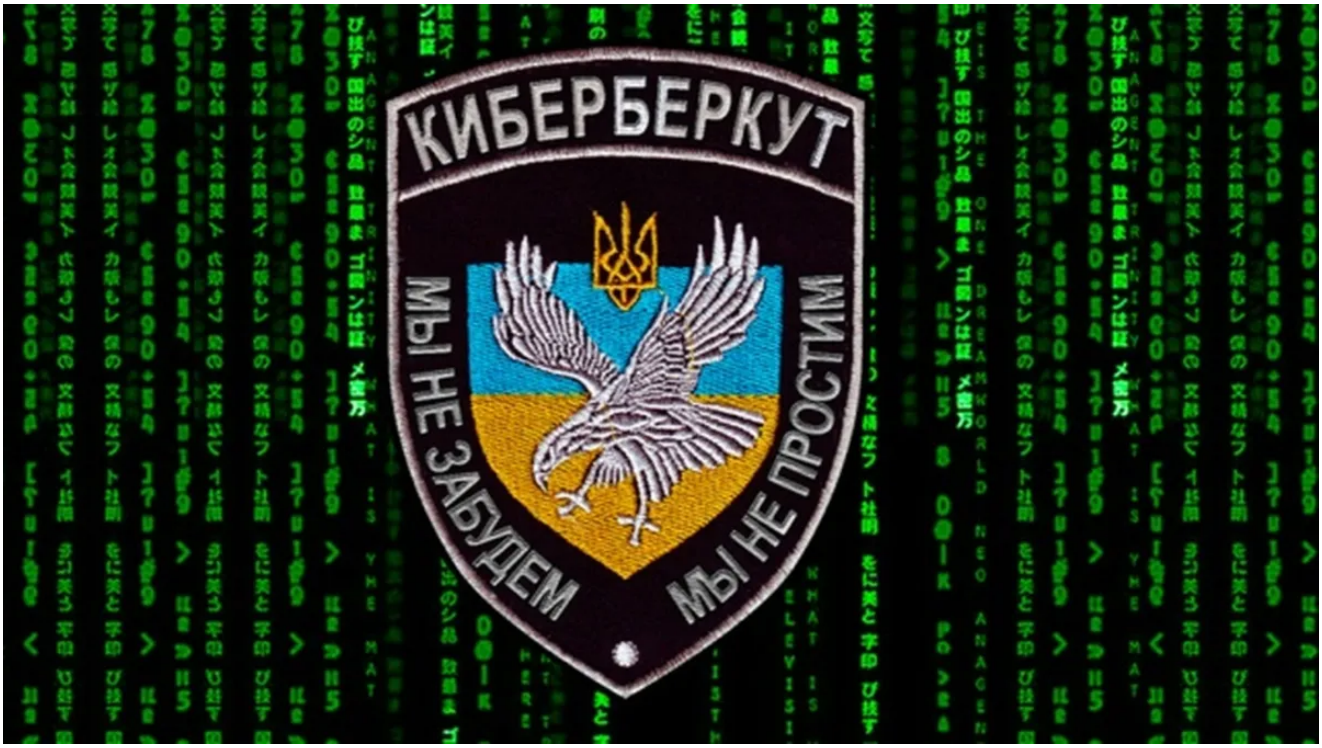
Understanding Uncertainty while Undermining Democracy

pylos.co/2020/09/23/understanding-uncertainty-while-undermining-democracy/

Joe 09/23/2020



Several US government agencies shared a warning on 22 September 2020 with respect to foreign entities using disinformation to sow confusion and discord around the US 2020 election. While evaluating this alert, Thomas Rid highlighted two key passages:

> **FOREIGN ACTORS AND CYBERCRIMINALS LIKELY TO SPREAD DISINFORMATION REGARDING 2020 ELECTION RESULTS**
>
> The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness of the potential threat posed by attempts to spread disinformation regarding the results of the 2020 elections. Foreign actors and cybercriminals could create new websites, change existing websites, and create or share corresponding social media content to spread false information in an attempt to discredit the electoral process and undermine confidence in U.S. democratic institutions.

and:

> The FBI and CISA urge the American public to critically evaluate the sources of the information they consume and to seek out reliable and verified information from trusted sources, such as state and local election officials. The public should also be aware that if foreign actors or cyber criminals were able to successfully change an election-related website, the underlying data and internal systems would remain uncompromised.

The central thesis of the document and the two highlighted passages above is that underlying election *integrity* may be unaltered and safe, but *communications* about such activity may be modified, obscured, or perverted for malicious purposes. As argued earlier here, many types of critical infrastructure attacks need not produce a substantial disruptive event – they only need to create a perception of unreliability or frailty to achieve significant impacts. As outlined above, the US government is clearly adopting this perspective and incorporating it into their risk framework for likely impacts to the 2020 elections.

Under this scenario, a likely attack could take the following route:

1. Anticipate a highly-contested, close election (which is almost certainly likely in the US).
2. Disrupt or interdict legitimate media communication surrounding election results as they are reported.
3. Leverage this disruption to push a variety of false or misleading narratives to sow doubt and confusion.
4. Once "regular" avenues of reporting are restored, sufficient doubt exists that election results are called into question by a noticeable portion of the population.

This may seem far-fetched, but as Mr. Rid pointed out in his book Active Measures, such a scenario has in fact already manifested – in Ukraine's 2014 Presidential elections. In this scenario, election authorities were repeatedly disrupted, with attackers ultimately interdicting official election result announcements – which were subsequently amplified by Russian state media.

In this specific case, Ukrainain defenders (as they have proven multiple times over the past decade) were up to the task in defending networks and rapidly restoring operations. But the direction of this attack – disrupting not only election operations, but election *communications* – highlighted fault lines that exist not only in Ukraine but in every modern democracy. Essentially, disrupting the actual machinery of modern elections – with its various systems, physical safeguards, and other checks – is quite hard. This is especially the case for a country as large and diverse as the United States, where there are essentially 50 separate authorities running national elections.

Instead of trying to either take the difficult route of modifying results or impacting individual precincts and districts piecemeal, a shortcut exists which CyberBerkut realized in 2014: target the transmission of results, rather than the results themselves. In hotly contested

elections – such as Ukraine's 2014 election or the US's 2020 Presidential election – audiences will eagerly demand results on election night, logistics and practicalities be damned.

In the case of federal entities such as the US, the combination of distributed election authorities, tightly contested races, and the contingencies put into place due to COVID-19, a very unique situation emerges. The following criteria likely hold for US elections in 2020:

- Ballots will be cast in a variety of formats depending on jurisdiction due to the impact of COVID-19, almost certainly resulting in a substantial increase in mail-in and absentee ballots.
- Current law in nearly all jurisdictions prohibits counting mail-in and similar ballots before the actual federal election day.
- Assuming the contest between Donald Trump and Joe Biden (along with multiple legislative and other positions) is close, delayed ballot counting will play a substantial role in deciding the outcome of elections.
- A populace generally attuned to knowing election results at the close of election day will be uniquely susceptible to messaging around results (or manipulations thereof) given delays and other artifacts surrounding current circumstances.

Based on these observations, the 2020 US election is an ideal opportunity for malicious actors to attempt various strategies to sow discord and dissent – not through modification or manipulation of any election results, but rather through disinformation and messaging modification.

While such activity may not manifest itself as bluntly as CyberBerkut's operations in Ukraine in 2014, the rough playbook from that event still holds. Only in this case, the electoral system in the US is *already* disrupted by events and the doubts generated by authorities (no less than the President himself) and various media outlets. So all an attacker need do in this situation is ensure a false or misleading narrative is published and disseminated widely in conjunction with "legitimate" results to sow significant discord and discontent in the US process. Given the already fraught nature of the current US election cycle, a mere "nudge" towards chaos may produce outsized results.

The most alarming aspect of the above scenario is that there is almost nothing that can be done to counteract it at this time. The surest means to combat disinformation – an educated, questioning, and alert public – is something almost beyond recognition given that the US populace is still unsure whether or not wearing masks might be a worthwhile consideration to slow the spread of COVID-19. When such relatively basic items meet such resistance, trying to convince individuals or groups that the narrative most sympathetic to their existing worldview may be false seems a daunting if not outright impossible task.

Ultimately, malicious entities need not compromise voter databases or election systems to sway or disrupt the US political process. A sustained, coordinated media campaign usurping already-degraded mainstream channels could very well succeed in pushing narratives that a vocal minority of the US population will embrace, leading to significant post-election chaos. And given the state of matters within the US and its extreme polarization, there is probably almost nothing that can be done to mitigate against this threat short of shutting down the internet and muzzling the press.

Given the above, I am deeply concerned and honestly quite afraid of what November 2020 will bring as of this writing. The preconditions for slight “nudging” existing prejudices to foment outright chaos or conflict already exist. Adversaries are not stupid, and have realized this. The open question at this time is not whether such adversaries will try to sow chaos in the US this year, but rather whether they understand US culture and divisions well enough to succeed in doing so.