All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The very real potential for rapidly escalating cyber conflict leading toward ...

The indications are that a seriously and rapidly escalating cyber conflict between the US and foreign governments (Russia, China, Iran, N. Korea, possibly others) will take place in a relatively short time frame. Perhaps days to weeks.

This not to be confused with the relatively minor events taking place today with ransomware.

What are the indicators?

The obvious indications related to the current published attacks show escalation, apparently with permission and support of governments. But what else is going on?

- The Executive Order signed by Biden was likely rushed out earlier than it was ready, indicating they have substantially accelerated their time frame for defensive action.
- The US President scheduled an in person meeting with Putin in a relatively short time frame.
- The US government has recently announced in no uncertain terms that all US businesses should take steps against these attacks and identified specific actions to be taken.
- The disinformation campaigns of Trump, Flynn, and others are pushing toward and setting time frames and expectations for putting Trump back in office in a few months.
- Previous attacks (e.g., Solar Winds) has left many Trojan Horses and remote access Trojans (RATs) still likely undiscovered and present.
- Actions by technical mechanisms and influence operations appear to be testing capabilities already in place as well as placing more capabilities into systems.
- Attacks have focused increasingly on critical infrastructures with no apparent immediate US response.
- The media is picking up the pace of speculations, leaks, and former officials discussing offensive US capabilities and how they might be legally applied and enabled.
- There are more in the technical realm, but I will ignore these for now.

What do they indicate?

Indications without warnings are like detection without response. Informative but with no effect. But that's not what we see here. The US government is issuing warnings, like the release of information requesting companies to defend themselves in specific ways. They may not have the word "WARNING", but they are warnings with specific actions associated. That, and the accelerated time frames, and published dates for outcomes related to historical precedents (e.g., Trump telling the Russians to proceed and they did as an analogy to Trump declaring August he would be back in the White house), cannot reasonably be ignored as coordination for events to take place soon and at larger scale than last time.

It seems apparent that the US will not stand by and let this happen like it did in the previous administration. The fact of rapid actions in the US government is generally not just associated with a change of management. It is typically associated with a level of urgency that means real actions are likely to happen soon. The whole of government approach to cyber-security, the multiple government intelligence agencies all coming out with versions of the path forward in a very short time frame, and the apparently more open communication of DoD components are all indicators of serious action in a short time frame. Then we have the intelligence information relating to White Nationalists being the greatest threat to National Security, and treatment of cyber attacks on the same footing as terrorism, leading to a reasonable conclusion that action is coming in an escalated form from the US and soon.

The threats are also on a tight time schedule, as the many changes being suggested and asserted will tend to weaken their previous positions in US systems and infrastructure. They are currently testing and verifying their capabilities, but they are also likely losing some of the really large scale capabilities they gained from inaction over the past years. So Russia and China and others will not want to wait as they are weakened and the US is strengthened. The Biden moves toward bringing more independence to the US in terms of supply chain are also things that will weaken the leverage of other countries over time. Thus they cannot simply wait and have their capabilities degraded by possible changes.

The underlying question seems to me to be whether, to what extent, and how the situation escalates and/or then deescalates. It is important to note that informational action does not necessarily imply only informational response. Cyber includes physical mechanisms, informational mechanisms, influence operations, and more. It seems likely that the physical nexus and operational technology (OT) effects are likely to result in physical response as well as other influence and informational domain actions. Economic sanctions combined with blowing up a Russian pipeline or two might help convince Russia to back off. And the demonstration against Russia might back off other countries. Note that Russia is also making physical; moves against its neighbors, and this may be the way they choose to occupy the US while taking military steps, or to back the US off of defending its allies. There are also indications of China and Russia cooperating, but these are far less clear, and it’s certainly unclear whether China would want to get involved in such an activity.

The strategic potentials

There are often unique points in time when dramatic shifts can take place. In the US, this is perceived by the World as one of them. There is the distinct possibility that this is the only opportunity for the next 50 years to flip the US from a democracy to an autocratic form of government. As such, it’s worth Russia taking the chance, particularly with Putin facing economic and social problems at home. He may view this as the unique opportunity to distract the US and take back a few neighbors, or working with China, they may see this as the opportunity of a generation to break the grip of the Western nations on the future of the World. Translated into global politics, this has the potential to turn insurrection into takeover.

Conclusions

When someone tells you they are going to try to do something, you should believe them. Indicators are signals that tell you what people are doing and planning to do. This report should act as a warning of the potential conflict about to escalate, and the potential for it to run out of control. You are warned. Take the warning seriously and act to protect yourself.

