Monthly Insights

June 2015

WIKISTRAT™
CROWDSOURCED CONSULTING

During the month of June, Wikistrat ran several simulations and forums exploring ongoing global trends and events. The following insights were gathered during those activities.

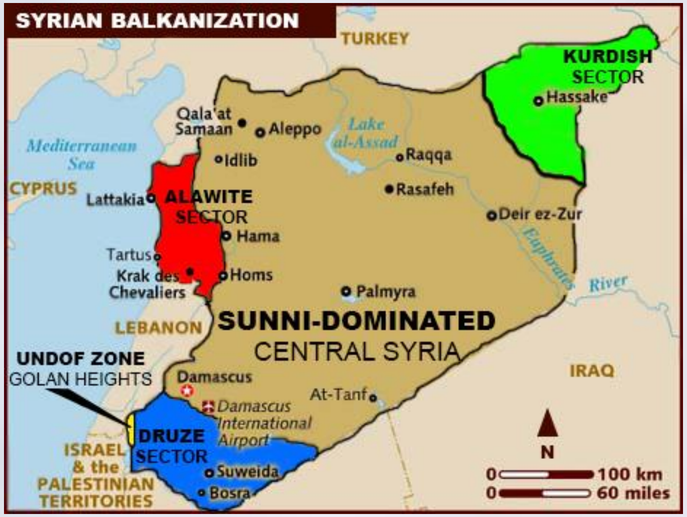
Insights from the "Day After Assad" Simulation

June 2015

WIKISTRAT™
CROWDSOURCED CONSULTING

There is no longer any peaceful way to keep Syria together

The West's largely hands-off approach to Syria's civil war has essentially doomed it to a violent conclusion. "Leading from behind" has kept U.S. troops off the ground in Syria, but the now-lengthy conflict has drawn in so many local players – all willing to fight to the bitter end – that Syria has little to no chance of ever resuming its status as a coherent nation-state. The much-feared re-drawing of the Middle East's colonial-era borders is now in full swing – to the regret of everyone but ISIS and the Kurds.



The Day After Assad

Without a decisive military intervention by outside powers, Syria will continue hardening into three de facto statelets – presaging the same for Iraq.

Much of Syria has already entered the post-Assad era, even as the strongman remains impressively secure in what is becoming an Alawite rump state in the West. Assad's forces have held off the rebel coalition, but in doing so, they have effectively ceded the rest of Syria to ISIS and Kurdish control. The Kurds in the north, ISIS in the East, and Assad's regime will all continue taking turns to indirectly aid one side while attacking the other, but none of the three can impose its will on the other two – which Syria's Kurds do not even aspire to. Syria's devolution is symbiotically linked to Iraq's on all scores: Iraq's Kurdish Regional Government spots an opportunity for expansion and *de jure* independence through absorption of Syria's Kurdish north; ISIS rules the Sunni heartland that connects the two states' landlocked interiors; and Tehran is the backstop sponsor for the co-religionist rump states (Alawite Syria, Shiite Iraq) that remain. Syria's non-ISIS rebels may well topple Assad in the long run, but that is unlikely to measurably change the correlation of sub-national forces. Whether the outside world cares to admit it or not, Syria's civil war has already arrived at its destination.

The most likely multinational intervention force can geographically widen the Syrian conflict, but it cannot decisively end it

Syria's moment to command the West's strategic attention has come and gone, leaving any additional military intervention to the two regional powers that knowingly enabled ISIS's rise in the first place – namely, Saudi Arabia and Turkey. Neither appears particularly confident right now, with Riyadh experiencing little but frustration in its Yemen military intervention and Recep Erdoğan's ruling AKP now humbled by its national elections setback. Even if such a coalition can be assembled, its overt entrance would only force Iran and its ally Hezbollah to redouble their own efforts while putting Washington in the awkward position of having to choose sides in an increasingly regionalized Sunni-Shia conflict. If the Saudis are looking to torpedo any U.S.-Iranian nuclear deal, however, these risks might well be justified.

The Kurds are the only true winner in this fight

So long as the war drags on, Syria’s Kurdish north enjoys de facto independence, while any peaceful settlement would likely grant it a subnational autonomy on par with the KRG in Iraq. The Kurds will proclaim their statelet as a prelude to union with the KRG both if the rebels unseat Assad, and if Assad survives. And the longer ISIS draws fire from all sides, the more time the Kurds have to cement their autonomy, much as the KRG did in Iraq between the first and second Gulf Wars. The only thing that might thwart the Kurds’ advance toward freedom is a major, Western-led military intervention, but that is not in the offing. In short, Kurdistan is a done deal. It is now simply a question of time and diplomatic recognition.

Lesser Syria = Greater Lebanon?

Hezbollah and Iran obviously lose in any Assad fall, because it threatens to eliminate key supply lines between the two. But if Syria is destined to be reduced to a de facto rump state, the question becomes, how can Tehran best maintain its grip on this western outpost of the Shia Crescent? Having already expended significant blood and treasure in its boots-on-the-ground support of Assad, Hezbollah will want something to show for all that effort, which may well end up being its quiet penetration of and control over any post-Assad Alawite regime that manages to survive Syria's breakup. Syria has long dominated Lebanon's political system to Hezbollah's benefit, so this "shotgun wedding" may be the most realistic pathway to keeping that Tehran-Damascus-Beirut axis intact.

Insights from the “Australia Taking the Lead” Forum

June 2015

WIKISTRAT™
CROWDSOURCED CONSULTING

Australia's economic reality predicts close ties with China

In some ways, Australia is Russia-lite when it comes to China's trade requirements: lots of untapped, uninhabited land, and natural resources far beyond its domestic needs. So of course Australia gets sucked into Beijing's economic orbit, and that rising trade interdependence makes the West all the safer because it attaches consequences to any Chinese belligerence – a brake Moscow does not provide.

The false choice between security and trade

History says trade follows the flag, meaning security relations between nations determine their economic ties. But in globalization, that dynamic is reversed, as trade leads and the flag reluctantly follows – China being the great example. Canberra cannot choose between its most important security ally (the U.S.) and its economic future (trade with China); it can only balance those two imperatives. So Australia is deepening its already close security ties with the U.S. while simultaneously joining China's Asian Infrastructure Investment Bank (AIIB) as a founding member. This is the essential yin-yang balance of Australia's foreign affairs.

How much can Australia play regional "balancer" on its own?

While the Australian public demonstrates a genuine willingness to increase its defense budget, the nation's armed forces are far from capable of projecting military power across the vast Indo-Pacific Region due to the "tyranny of distance" – Canberra's longtime lament on security matters. That doesn't mean Australia lacks options. It was the second nation after the U.S. to sign a security pact with increasingly nervous Japan, and there are compelling reasons for Canberra and New Delhi to increase their security cooperation. But Australia's sometimes tense relations with Indonesia (the world's most populous Muslim state) demonstrates the limits to this approach. Australia will always be viewed by other Asian powers as belonging to the "whites only" club – the so-called Five Eyes group that features intelligence sharing with New Zealand, Canada, the U.S., and the U.K.

The logic of playing "launchpad" to the U.S. strategic pivot

As the longtime champion of the Responsibility to Protect (R2P) logic of humanitarian interventions, Australia enjoys a relatively benign security reputation across Asia (its tensions with Indonesia over East Timor notwithstanding). That reputation, combined with the "tyranny of distance," makes Australia the natural choice – compared with too-close Japan or South Korea – to host any build-up of U.S. strategic power as a counter to rising Chinese militarism. With Beijing deep into actualizing its anti-access, area denial (A2AD) military strategy, any such buildup should logically emphasize air assets over naval ones. Australia is the perfect "stand-off" platform for the stabilizing the U.S. pivot, and it should embrace that role for the sake of the rest of Asia's small and medium powers.

Insights from the “Space Control in 2030” Simulation

June 2015

WIKISTRAT™
CROWDSOURCED CONSULTING

Space Control in 2030

- **Space control need not involve space ships exchanging salvos.**
  - The major military benefit of space systems is to provide force-multiplying information to ground-based combatants.
  - Space control in 2030 will principally comprise attacking and defending the ability of these systems to provide such information, both in space and on the ground.
- Just as with information warfare, **deterrence may not be limited to the space domain**.
  - Retaliation will likely be directed at whatever domain the adversary most depends on.
- Cyber (or other) attacks on **ground infrastructure** may be more widely available – and perhaps more effective – than attacks on space segments.
- **There is an asymmetry between the value of space assets to conflict and the need to protect them.**
  - The U.S. will engage in expeditionary combat, while opponents will be on or near their home turf.
  - Satellites therefore have a higher value to the U.S., which has a greater motive to dissuade or repel attacks.
- **Defense must go beyond making satellites more resilient**; it must include making ground segments more resilient as well, and improving attack detection.

Insights from the “The Rise of the Cyber-Mercenary” Simulation

June 2015

WIKISTRAT™
CROWDSOURCED CONSULTING

State employment of cybermercenaries will grow explosively in near term

In a world of great powers seeking to organize their regional spheres of influence, cyber operations have become a leading soft-power asset on all levels: great powers targeting other great powers or smaller states, and weaker states defending themselves against greater ones. For now, all this online activity is treated as an adjunct or – more dangerously – a prelude to traditional warfare, but as the reach, impact and sophistication of cyber operations increase, governments and their militaries are highly incentivized to capture these activities by putting hackers in uniform.

Growing cyber brinksmanship eventually triggers cyber deterrence

States will attempt in vain to monopolize this virtual “violence”, but the effort will come to redefine traditional state-on-state war (as seen in Russia’s hybrid/irregular warfare against Ukraine). Eventually, enough lines will be crossed that one state’s cyber operations will trigger the opponent’s kinetic responses – something already written into U.S. national strategy. When that shift unfolds, it will be akin to the 1962 Cuban Missile Crisis and its codification of the doctrine of mutually assured destruction, in that it will force mutually vulnerable states to find a common definition of cyber deterrence. The effort to detail the “laws” of cyber warfare will proceed fitfully and slowly at first, but culminate quickly after a particularly disastrous conflagration.

Insurgencies will increasingly virtualize themselves through cyber operations

As states embrace pervasive sensoring of urban environments and infrastructure, it will become harder and harder for insurgents to wage kinetic forms of asymmetrical warfare in advanced economies. These same networks, however, will prove rich in targets for the offensive cyber operations of insurgencies that do adapt. The ultimate target is always the state’s popular legitimacy, which can be accomplished quite efficiently through cyber attacks on government installations, hacking election machinery, misinformation campaigns on social networks, industrial espionage and sabotage designed to sour an investment climate, and so on. Moreover, such insurgent cyber operations offer direct participation for sympathetic expatriates, rather than mere financial support. Virtual insurgencies are thus naturally transnational in scope.

Private-sector cyber operations will be far harder to curtail

All governments generally adhere to the realist notion that an opponent’s survival as a functioning state – however compromised – is preferable to its complete collapse, leaving costly chaos in its wake. Private-sector enterprises, on the other hand, actively seek their competitors’ demise in true zero-sum fashion. Almost any offensive cyber operation is considered fair game, albeit through third-party contractors (formal economic mercenaries) due to liability or criminal-prosecution exposures. Government involvement on behalf of state enterprises or flagship companies will be almost totally unrestricted – up to the point of triggering physical damage or encroaching on national security firms. This competitive zero-sum landscape, accentuated by the leveled playing field of globalization, will hamper cooperation among private and public enterprises in suppressing truly criminal cyber operations by organizations seeking strictly monetary rewards.

The Rise of the Cyber-Mercenary

Survive the age of unrestricted cyber warfare by accepting certain realities

- The rise of digital currencies will destabilize their real-world predecessors until regulatory regimes are constructed in response to their displayed capacity for economic disruption.
- The Deep (hard to search) and Dark (hard to access) portions of the Web are the “sea” in which cyber mercenaries, terrorists, criminals and hacktivists swim. Taming this environment will take decades – if it can be at all achieved.
- The degradation of trusted media sources by nefarious cyber actors has already resulted in a growing culture of conspiracy thinking that threatens the legitimacy of all states, both the pluralistic and authoritarian. If anything, this growing popular mindset favors oppressive governments better at hiding their weaknesses than free states, which are more open about their faults by design.
- Cyber forces are becoming the new clandestine services of nation-states, triggering an era of dangerous experimentation akin to the early years of the nuclear age. The world will not grasp the need for mutual definitions of strategic cyber deterrence until great destructive capacity is demonstrated. Cyber variants of World War II’s nuclear strikes on Hiroshima and Nagasaki are inevitable.
- As states increase their cyber arsenals, recruitment of “foot soldiers” will grow increasingly sophisticated. Today, it is often a matter of co-opting “black hat” hackers into “white hat” service personnel. Over time, prodigies will be groomed from their childhood onward, lured by the promise of waging cyber wargames for real. The science-fiction classic *Ender’s Game*, which predicts this pathway, has had enormous influence over the U.S. military establishment, in turn setting the gold standard for the rest of the world’s militaries.