SPOOKY ASSADLEAKS: THE PROVENANCE OF THE EMAILS

As I wrote in this post, I got interested in the provenance of a set of leaked Bashar al-Assad emails largely because of the way in which two of them were used to suggest, dubiously, Nir Rosen was an Assad agent.

The Guardian and Al Arabiya have both offered posts describing, in part, how they came by the emails, with the Guardian's offering more details. The short version is:

March 15, 2011: Uprising escalates in Daraa.

Late March: "a young government worker in Damascus" handed off a slip of paper to a friend. The paper had four codes (plus or including the two email addresses, the Guardian is not clear) that would provide access to personal email accounts of Bashar al-Assad and his wife Asma. The friend was apparently supposed to pass them onto "a small group of exiled Syrians who would know what to do with them."

June: "Two Syrian professionals in a Gulf state" obtain the emails. The Guardian doesn't explain whether they were the original intended recipients, nor does it explain the delay. Though it does include a blurb describing their sudden awakening to politics that makes it clear the Guardian has spoken to at least one of the activists and replicated their self-narrative uncritically.

> The uprising in the southern Syrian city of Deraa on 15 March had empowered them, as it had hundreds of thousands of others in the totalitarian state. They were now determined to do what they could to bring an end to more than four decades of rule by the Assad clan.

> “It was clear who we were dealing with,” said one of the activists. “This was the president and his wife. There was no doubt.”

August 6: Sabu solicits Syrian MOD hacker to “disrupt govt communication systems.”

June to December: The emails are used with increasing frequency over time; Assad appears to build a PR strategy using them.

January: Anonymous (which had been infiltrated by the FBI since at least June, the same month the Syrian activists purportedly got the email codes) hacks Bashar al-Assad’s servers, accessing 78 different email accounts.

February 7: Anonymous releases the Assad emails which were published by Ha-aretz, claims the password was 12345. These are, at least in part, the very same emails being released today. Assad’s brother-in-law Firas al-Akhras emails him to tell him the inbox of the Ministry of Presidential Affairs had been leaked. All the emails are shut down.

March 15, 2012: The emails published.

In their narratives, neither the Guardian nor al Arabiya note that the FBI had been running Sabu since last June, precisely the same month the “activists” reportedly got the “secret codes” (12345?) that would allow them to access the Assad emails.

Now there are plenty of questions I have about this: Who was the mole, how did he or she get this information, who was the friend, what caused the 3-month delay. All of those questions, of course, are particularly interesting giving the coincidence of timing with the Sabu recruitment.

And why release these emails now? Just because of the one-year anniversary of Daraa, and the other events planned for the day?

Suffice it to say it feels a lot like outside

entities—aside from whatever professionals-turned-activists purportedly monitored these accounts—were involved.

With that feeling in mind, two more details worth noting. First, al Arabiya's story on how they got the emails focuses instead on what they didn't publish: a bunch of "scandalous emails."

> Hundreds of "scandalous" emails were accordingly deleted by Al Arabiya.

By comparison, the Guardian said only it didn't publish personal emails. Both sources, however, want people—perhaps including Assad?—to know that there were more emails that may be out there.

The other thing I find interesting is the detail the Guardian pays to Assad's email habits.

> [The Syrian activists in the Gulf state] soon noticed differences in the way the couple used their email accounts. "We had to be quick with Bashar's emails," one of the activists said. "He would delete most as soon as they arrived in his inbox, whereas his wife wouldn't. So as soon as they went from unread to read we had to get them fast."
>
> Deleting emails as soon as they arrive shows a degree of awareness of web security. So too did the fact that Assad never attached his name or initials to any of the emails he sent. However, many of the emails that arrived in his inbox are addressed to him as president and contain intimate details of events and discussions that were not known outside of the inner sanctum and would have been very difficult to manipulate.

Even before I remembered that the same guy the Guardian claims was showing some web security used "12345" as his password, this entire passage sounded bogus, more like a way to

provide cover for some other means to collect these emails that don’t involve more sophisticated wiretapping of packets, as opposed to email in-boxes.

But once you remember this is a guy who reportedly used “12345” as his password, then the entire claim Assad was practicing good security becomes laughable. Which makes this entire passage suspect.

There are two stories of how Bashar al-Assad got his emails hacked in the last year. In one version, Syrian activists managed to spy on their dictator in real time and are presumably releasing emails that lack a smoking gun (but did include “scandalous” emails) as a sort of anniversary present for Assad. The other story involves the FBI flipping at least one hacker and having him continue to hack at their command.

Or maybe there’s just one, far more intriguing story.