GlobalResearch
Center for Research on Globalization

Dotty Domains: The Pentagon's Mali Typo Leak Affair

By Dr. Binoy Kampmark
Global Research, July 26, 2023

Region: Europe, USA
Theme: Intelligence

***

Fleet-footed agility and sharp thinking rarely characterise the plodding bureaucrat. An argument can be made that different attributes are prized: cherished incompetence, spells of inattentiveness, and dedication to keeping things secret with severity. What matters is not what you did, but what you pretended to do.

Even with maintaining secrecy, the plodding desk-job hack can face problems, all falling under the umbrella term of "human error". Papers and files can stray. The occasional USB stick can find its way into unwanted hands. And then there is that damnable business about the cloud and who can access it.

Despite repeated warnings over a decade by the Amsterdam-based Mali Dili, contracted to manage email accounts of the West African state, traffic from the US military continued to find its way to the .ml domain, the country identifier of Mali. (For all we know, this may still be happening.) This arose because of a typing error, with .mil being the suffix for US military email addresses.

Other countries also seemed caught up in the domain confusion. Over a dozen emails intended for the Dutch military also found their way into the Mali Dili net, with .ml being confused with .nl. Eight emails from the Australian Department of Defence, intended for US military consumption, also met the same fate. These include problems about corrosion in Australia's F-35 and an artillery manual "carried by command post officers for each battery".

The man most bemused by this is not, it would seem, in the Pentagon, but a certain Dutch entrepreneur who was given the task of managing the domain. Johannes Zuurbier has found himself inconvenienced by the whole matter for some years. In 2023, he decided to gather the misdirected messages. He currently holds 117,000 of them, though he has received anywhere up to 1,000 messages a day. He has been good enough to badger individuals in the US national cyber security service, the White House, and the local defence attaché in Mali.

The *Financial Times* reports that the contents of such messages vary. Much of it is spam; a degree of it comprises X-Rays, medical data, identity documents, crew lists for ships, staffing names at bases, mapping on installations, base photos, naval inspection reports, contracts, criminal complaints against various personnel, internal investigations on bullying claims, official travel itineraries, bookings, tax and financial records.

While not earth shaking, one of the misdirected emails featured the travel itinerary of General James McConville, the US Army's Chief of Staff, whose visit to Indonesia was noted, alongside a "full list of room numbers", and "details of the collection of McConville's room key at the Grand Hyatt Jakarta." Not the sort of thing you necessarily wish your adversaries to know.

Another email from the Zuurbier trove came from an FBI agent and was intended for a US Navy official, requesting personal information to process a visitor from the Navy to an FBI facility.

Lt. Commander Tim Gorman, a spokesperson from the Office of the Secretary of Defense, has put a brave face on it. "The Department of Defense (DoD) is aware of this issue and takes all unauthorized disclosures of Controlled National Security Information or Controlled Unclassified Information Seriously," he outlined in a statement to *The Verge*. He further claimed, without giving much away, that emails sent from a .mil domain to Mali are "blocked", with a notification being sent to the sender "that they must validate the email addresses of the intended recipients."

To keep things interesting, however, Gorman confesses that there was nothing stopping other government agencies or entities working with the US government from making the mistake and passing on material in error. His focus, rather, was on the Pentagon personnel, who continued to receive "direction and training". The Defense Department "has implemented policy, training, and technical controls to ensure that emails from the '.mil' domain are not delivered to incorrect domains."

The whole affair is becoming a thick parody of administrative dunderheadedness. It follows a pattern of inadvertent exposure of data, the sort that would, if published, probably lead to harassment and prosecution by the Department of Justice. But the incompetent are almost never found wanting; only the well-intentioned deserve punishment. Instead, IT misconfigurations are blamed for what happened, for instance, in February, when three terabytes of US Special Operation Command unclassified emails were made available for public consumption for some two weeks.

Even as the typo-leaks continue, the United States has imposed sanctions against, of all individuals, Mali's own defence officials, including the defence minister, Colonel Sadio Camara. The two other individuals in question are Air Force Chief of Staff Colonel Alou Boi Diarra and Deputy Chief of Staff Lieutenant Colonel Adama Bagayoko. In one of his tedious moral fits, US Secretary of State Antony Blinken accused the trio of facilitating and expanding "Wagner's presence in Mali since December 2021", claiming an increase of civilian fatalities by 278 percent since the Russian mercenary group established itself in the country.

The Mali authorities, as of July 25, should have assumed control of the domain. This worries retired US admiral and former director of the National Security Agency and US Army's Cyber Command, Mike Rogers. "It's one thing when you are dealing with a domain administrator

who is trying, even unsuccessfully, to articulate the concern. It's another when it's a foreign government that … sees it as an advantage that they can use."

Zuurbier, at the conclusion of his decade-long contract, may still have a few juicy numbers for safe keeping, though he will be mindful about what happens when such contents are published, namely, the Assange-WikiLeaks precedent. Mali's officials, in the meantime, will simply anticipate the dotty domain business to continue.

*

Note to readers: Please click the share button above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He currently lectures at RMIT University. He is a regular contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

Featured image is from TruePublica
