

Security as Diplomacy: Owning Our Own Capacity in the Caribbean

Oct 12, 2026 · @Felicia Ellis

Prepared for His Excellency CoP (Ret'd) Ian M. Queeley, CSM, Ambassador & Head of Mission, Embassies of Eastern Caribbean States to the Kingdom of Morocco, RSS and UWI Caribbean Security Futures Symposium, Barbados, October 2026.

Part One: The View From Above

When I fly a drone over a coastline, I see what the beach hides. I see the shipping lanes, the cables, and the places where many paths meet. This report starts from that high view, then zooms in.

From above, three things stand out.

1. **More ships are passing through our waters.** Global oil strategy moves tankers through the Caribbean Sea. More ships mean more chances for accidents and more attention from powerful nations.
2. **Our internet runs along the ocean floor.** Most of the world's internet traffic travels through undersea cables. Many of those cables pass through Caribbean waters. A dragging anchor, a fishing net, or a deliberate act can cut one. When it breaks, an island can lose its link to banks, hospitals, police radios, and families.
3. **Space is becoming infrastructure.** Satellites now carry internet and communications across the globe. Companies such as Starlink offer this service, and more countries see it as backup. That is good. It also raises a question every nation must answer: who controls the backup?

Put those views together. Our island nations need a way to stay connected when the seabed is cut. They need that connection without giving up control of their own security.

Part Two: What Sovereignty Really Means

Sovereignty is not isolation. No island can build every cable, satellite, and data center alone. Sovereignty means three things:

1. **We decide how our security data is handled.**
2. **We have people who can run, check, and challenge the technology we use.**

3. We own some of the capacity, so no single outside company can switch us off.

The chip industry shows the pattern. The leaders did not start with factories. They started with people. They trained engineers through universities and apprenticeships, then built the factories. The people came first, then the ownership.

Who Sets the Rules? The Frontier AI Accord

On September 29, 2026, executives from six frontier AI companies signed the White House Accord on Super Intelligence. The signers were Google, Anthropic, Meta, OpenAI, xAI, and Nvidia. Most of them lead the field, so the list shows who Washington considers building at the frontier.

The accord asks each company to do four things:

1. Monitor its models during training and deployment, including for cybersecurity, biosecurity, and chemical threats.
2. Keep an internal team to make sure those controls work.
3. Hire an independent outside auditor to check them.
4. Give a board committee oversight of the reports.

It is voluntary. It has no penalties and no regulator. Its authors say these steps may later become law, but the accord does not require it.

Why this matters for us: a voluntary accord is a statement of intent. It works only if the companies keep their word. The same question applies to every island nation: who sets the rules for the tools we depend on, and what happens if they change them? That is the sovereignty question again, one layer up from satellites and data.

Part Three: Our Recommendation

Build the talent now. Own some of the capacity next.

1. **Talent.** Create regional cohorts of engineers, technicians, data protection officers, and policy staff. Begin with the Caribbean Compute Pilot, which already uses a talent-first model. The first cohort can focus on women, so young women see themselves in this work from day one.
2. **Shared access.** Pool compute and connectivity so small nations do not each buy the same expensive equipment alone. Negotiate group terms with satellite providers, with protections for data, local jobs, and service during a crisis.

3. **Owned capacity.** Over time, allied nations pool resources to own pieces of the infrastructure together. Examples include a regional ground station, a secure data center, or a small satellite program with partner launch access.

The Compute Pilot: Build the People, Then Secure the Compute

Start with 25 cybersecurity and law enforcement professionals. Then grow the cohort to 50, 75, and 100. Each step is one cohort. Each cohort has about five people in each of five tracks: SOC Analyst, Forensic Investigator, Threat Hunter, Human Trafficking Investigator, and Policy Analyst.

The path has four steps:

1. A data analysis foundation.
2. Security as Diplomacy certification.
3. A technical track.
4. A shared case exercise, where technical and policy participants work together on a regional problem, such as an undersea cable outage.

UWI is a prospective co-host. No compute partners are committed yet. Compute terms, funding, and governance are open for regional decision.

Who We Pursue and Why

These are targets, not commitments. Each one has a clear reason to care and a specific ask. Status is as of this report.

Partner	Why pursue	The ask	Status
RSS Secretariat (Rear Admiral Errington Shurland)	Regional security body for eight member-state police forces, with the security mandate	Sponsor the talent pilot and host the ownership conversation	Not yet contacted
CARICOM IMPACS (Lt. Col. Michael Jones)	The region's security coordination body and the natural home for shared capacity	Review the world lab concept and name a regional owner	Not yet contacted

Partner	Why pursue	The ask	Status
UWI (symposium co-host)	Universities produce the engineers and policy staff the talent track needs	Co-design the first cohort curriculum	Not yet contacted
Association of Caribbean Commissioners of Police (Marcia Manning)	Connects police leaders across islands and can carry the training use cases	Pilot the cable-outage and hurricane scenarios with commissioners	Not yet contacted
Allied governments and institutions (to be named)	Shared facilities, launch access, and funding no island can fund alone	Identify three partners willing to co-own a small capacity site	Not yet identified
Compute and satellite providers (AMD, Nvidia, satellite operators)	Hardware for training and backup connectivity	Ask about regional programs and group terms, as conversations, not deals	Not yet contacted

Who Is Building Their Own Space Internet

The plain idea: countries build their own satellite internet so they do not have to depend on someone else's.

The lesson from Ukraine

Starlink, SpaceX's satellite internet, became a lifeline for Ukraine's communications during the war. Russian forces also used Starlink terminals, some bought on the black market. In February 2026, Ukraine's defense ministry said Starlink terminals used by Russia had been cut off ([KRDO](#)). A senior Russian military official later acknowledged that the terminals had been disabled for about two weeks ([Anadolu Agency](#)). One company's decision changed frontline communications overnight.

Who is building their own

Country or bloc	Program	What it is	Status as of October 2026	Source
United States	Starlink (SpaceX)	The largest commercial satellite internet service. Its operator can switch terminals on or off.	Operating. Used by Ukraine and many other countries.	Wikipedia
Russia	Rassvet	A Starlink-style network. One report targets 292 satellites by 2027.	First 16 satellites launched in May 2026. A Euronews analysis says it has not yet worked well and still threatens Ukraine.	Euromaidan Press , Euronews
China	Guowang and Qianfan (G60)	Two large low-orbit internet networks.	Launches continuing. Batch 7 of Qianfan carried 18 satellites in April 2026, and another 18 launched on a Long March 6 in July 2026.	CISLUNAR , CISLUNAR
European Union	IRIS ²	A secure, multi-orbit satellite network. It serves both civil and defense needs and is operated by SpaceRISE.	Deployment accelerated in August 2026, with an expanded satellite count.	EUSPA

Dual use

The same satellite that gives an airline passenger Wi-Fi can also support military communications. That is why investors watch this market, and why public safety planners should watch it too.

The lesson for us

A country that does not own its space communications is renting its safety from someone else. This is the same lesson as sovereign AI and sovereign data, one layer higher.

The question for every government is simple: who can switch off our communications, and what happens if they do? Our partner conversations should start there.

Energy as Leverage

Whoever controls the fuel supply holds leverage. That idea runs from the Strait of Hormuz to Havana.

Cuba shows what happens when supply is cut. Reports say Cuba has run out of oil, with blackouts and protests spreading ([SAN](#)). Mexico, which had been sending fuel, has sought to restart shipments ([WTOP](#)). Cuba is about 90 miles from Florida, so what happens there reaches the whole region.

The Strait of Hormuz is the wider version of the same risk. A large share of global oil passes through one narrow channel, so disruption there raises prices for everyone, including small island states.

Did Venezuela's fall change the cost of disrupting Hormuz?

The question to test is this: if Venezuela's oil output is no longer available to a friendly government, does that change the leverage an adversary gets from threatening a shipping lane? The answer depends on evidence we still need: how much Venezuelan crude reaches world markets, how quickly it could rise, and how much Gulf supply can be replaced.

Until that evidence is in hand, this report treats the question as open.

Part Four: A Regional World Lab, Built for Security Only

Some of the newest AI tools learn from simulated worlds. These are called world models. They generate three-dimensional environments where machines and people can practice. A regional world lab would build those environments for security training and planning, owned by the region.

First use cases

- **A damaged undersea cable:** Simulate the outage, test backup routes, and train technicians and officials to respond.
- **A hurricane response:** Model flooded roads, damaged ports, and shelter logistics before the storm arrives.
- **A port security incident:** Train port staff, customs officers, and police in realistic scenes.

Guardrails

These rules belong in the foundation, not added later.

- **Security use only.** The model supports training, planning, and response.
- **No surveillance of citizens.** The lab does not track or profile people.
- **Data stays in the region.** Sensitive information is stored under regional law.
- **Human oversight.** A trained person reviews every high-stakes output.
- **Allied buyers only.** Access goes to partner governments that share these rules.

Ownership

A regional body, such as RSS or CARICOM IMPACS, or a nonprofit it designates, should hold the model and its income. Revenue from paid access should be reinvested in training and infrastructure, not sent out of the region.

Honest status

We do not yet have compute partners. Today this is a plan, not a finished lab. The path runs through allied governments, shared facilities, and vendor programs. I bring it to the symposium so the region can decide together whether and how to pursue it.

Part Five: The Zoomed-In Punch List

When the view from above is clear, zoom in on the next steps.

Next 30 days

- ☐ Review this report with Ambassador Queeley.
- ☐ Confirm the regional body that will sponsor the talent pilot.
- ☐ Identify three potential partner governments or institutions.

Next 90 days

- ☐ Draft the first talent cohort plan, with a curriculum on cables, satellites, and data protection.
- ☐ Write a one-page term sheet for group access with satellite providers, including data and jobs protections.
- ☐ Build one undersea cable outage scenario to test the simulation idea.

Next 12 months

- ☐ Stand up a shared compute and training site with at least one allied partner.
- ☐ Publish the guardrails as a regional standard.
- ☐ Decide the ownership structure for any owned capacity.

Part Six: The Ask

I ask the symposium for three things.

1. **Attention:** Keep undersea cables and satellite backup on the regional security agenda.
2. **Partnership:** Name the partners who will help build shared talent and capacity.
3. **Ownership:** Agree that any regional capability belongs to the region.

Security is not only about what we defend against. It is about what we build together. Let us build it on our terms.

Appendix: Verified Market Facts (as of October 12, 2026)

Unverified items are left out. Check Muse's current ranking before publishing.

Fact	Status	Detail	Source
AMD crosses \$1 trillion	Confirmed, intraday	First crossed September 21, 2026; one source closed just below	ROIC
AMD stock gain in 2026	Partly confirmed	About 175% by one source (about 2.75 times the start)	Pulse2
AMD buys World Labs	Confirmed	About \$8.2B all-stock; announced September 28, 2026; closing expected by end of 2026	SDxCentral
Meta and Scale AI	Confirmed	\$14.3B for 49% stake; \$29B valuation; announced June 12, 2025; voting terms not verified	Maginative
Cursor round dropped	Reported	About \$2B round reported dropped, April 2026; original Bloomberg report not opened	Texxr
SpaceX buys Cursor	Confirmed	About \$60B all-stock; announced June 16, 2026; closing reported August 14, 2026	Gigazine
Meta's Muse app	Confirmed for September 18 to 28	Launched September 8, 2026; No. 1 on U.S. App Store; today's ranking not verified	TechCrunch