EXECUTIVE SUMMARY

TCA Trustless Computing Association

Opportunity for like-minded States, Intergovernmental Organizations and NGOs to join as cofounder partners of the Trustless Computing Certification Body and Seevik Net initiative.

(version of February 28th, 2022)

The Trustless Computing Certification Body and Seevik Net initiative constitutes a **cybersecurity diplomacy and capability-building initiative** that is aggregating a critical mass of states, intergovernmental organizations and NGOs to jointly build and govern a new **global digital infrastructure for sensitive non-classified mobile computing**, a governance structure for its joint management, and mechanisms for their national and international *legitimate* lawful access.

The initiative aims to foster the wide availability of mobile IT systems with **radically unprecedented levels of both privacy and accountability** for the sensitive (non-classified or low-classified) mobile communications of tens of thousands and then millions of sensitive law-abiding citizens most targeted for profit and political reasons - from prime ministers to **diplomats**, from elected officials to businessmen, from journalists to activists - while running alongside current hegemonic mobile devices, apps and cloud services IT systems.

By April-May 2023, we are gathering a **critical mass** of no more than 3 EU nations, 4 non-EU diverse **globally-diverse** states and a few fitting NGOs and IGOs (like the EU, UN, African Union), to become the initial *cofounder partners* of such open inter-governmental joint-venture to build and govern the **1st global democratic digital communications infrastructure**, within the confines of current national and international laws and downward compliant to the highest applicable standards.

SUMMARY 3-PAGER

ABOUT US: Since 2015, the Trustless Computing Association, in **Geneva** and **Rome**, has been advancing the **Trustless Computing Certification Body and Seevik Net** initiative, via multiple activities, including 3 EU R&D programs and several publications together with 22 world-class R&D partners including two states, 25 top advisors, and a global conference series called Free and Safe in Cyberspace held in 8 editions on 3 continents, with over 120 world-class speakers to promote the same. In 2019, we created a *spin-in* startup, TRUSTLESS.AI, with a top team, advisors, and investors, to build initial minimalist TCCB-compliant IT systems - which is bound to be re-owned by the TCA/TCCB, as per the “spin-in” model.

WHAT: The Trustless Computing Certification Body and Seevik Net initiative is both (1) an **inter-governmental cyber diplomacy** initiative to radically or substantially increase the confidentiality, accountability and convenience of the sensitive non-classified mobile communications among diplomats, elected officials, prime ministers, and law-abiding citizens, within and across participating states and any state; as well as (2) an **inter-governmental cybersecurity capability-building** initiative that is bringing together a critical mass of states, IGOs and NGOs to build and govern a new global digital infrastructure for sensitive non-classified mobile computing, and mechanisms for their national and international *legitimate* lawful access.

COMPONENTS: The initiative entails the creation of: (1) the *Trustless Computing Certification Body* (TCCB), a new **inter-governmental IT security standards-setting, certification and governance body** established in Geneva last June 2021, and (2) *Seevik Net*, an initial set of TCCB-compliant mobile IT systems, ecosystems and solutions, based on transparency, neutrality, multilateralism, and time-tested democratic oversight and governance models, and open, globally-supported, battle-tested, low-level open IT platforms, based on **Sel4** operating systems and **Risc-V** processors.

SEEVIK NET: Seevik Net will include a multinational TCCB-compliant set of hosting rooms, messaging apps for mainstream mobile stores, and **2mm-thin mobile devices carried in custom leather wallets or embedded in the back of any global commercial smartphone**. Such a new mobile form factor and product class enables such systems to **conveniently complement today's hegemonic mobile devices**, apps and services that we've all grown dependent on, instead of trying to outright replace them.

COMPLEMENTARITY: The initiative aims to gradually **replace the current failed hegemonic model of reconciling personal privacy and public safety in mobile systems** - centered on chronically insecure devices and an obscure market of spyware and malware - with one that is much more effective in protecting both human rights and state security, as well as global security, public safety and trust within and among states.

UNIQUE SECURITY: TCCB and Seevik Net will achieve radically-unprecedented levels of trustworthiness (A) by applying to both **extreme, battle-tested, and open** (technical and organizational) **socio-technical safeguards, and checks and balances,** the Trustless Computing Paradigms, that are applied to all technologies and processes critically involved in the entire life-cycle - down to fabrication oversight, CPU design and hosting room access and (B) via a governance model and statute that highly maximizes global **democratic accountability**, socio-technical competency, and resiliency from state pressures.

GOVERNMENTAL & DIPLOMATIC USE CASE: It will especially benefit officials and staff of **prime ministers, parliaments, and ministries of foreign affairs and defence** as these are struggling with the huge scale and pervasiveness of illegal hacking of their personal smartphones, when the overwhelming majority of those **professional and personal associates** need to speak to about sensitive (albeit non-classified) matters do not have their classified phones or apps, or have incompatible ones.

While most states nowadays, for **internal** low-classification communications, mandate their staff use specific **enterprise/state** secure messaging apps and hosting (e.g. Wire, Matrix, Threema, Wickr,) and in some cases secured commercial phones - for **external** non-classified but sensitive communications they are increasingly suggested or mandated to use specific **consumer** secure messaging apps (e.g. Signal or Telegram), while **no app can be more secure than the device it runs on**, as we've learned.

CITIZENS USE CASE: It will be initially targeted for the **sensitive mobile communications of millions of law-abiding citizens**, elected officials, diplomats, journalists - and institutions and organizations - that are most targeted for profit or political reasons. Private market demand is very significant. Pre-Covid surveys by UBS and by Northern Trust show that even the 16 million wealthiest persons in the World and family offices regard **cybersecurity as their n.2 or their n.1 concern**, respectively.

BENEFITS: By leveraging **unique levels of transparency and inter-governmental cooperation** at all levels and stages - the initiative aims to (1) achieve radically unprecedented levels of actual and perceived trustworthiness by users and elected officials anywhere in the World; (2) advance **digital sovereignty radically and concurrently at the state, international and citizens' levels** and (3) enable and foster **confidential, fair and effective global dialogue** within and among states.

OPPORTUNITY: We are selecting **no more than 3 EU states, 4 globally-diverse non-EU states, 2 IGOs** (e.g., EU, UN agencies, Arab League) **and 2 neutral and fitting INGOs** (e.g. ICRC, Amnesty International) to become *cofounder partners* of the TCCB and Seevik Net initiative. *Cofounder partners* will enjoy temporary special privileges, including:

- (1) receive 900 mobile device units each;
- (2) be able to establish TCCB-compliant hosting rooms;
- (3) participating with their firms to the development rather than just oversight of Seevik Net;
- (4) participating in the initial TCB governance that will give shape to its statute and first operational version of the *Trustless Computing Paradigms*;
- (5) private and public entities headquartered in their territory will have exclusive access for the first 12 months (5.a) to purchase a TCCB-compliant IT system and (5.b) to submit IT services for certification from TCCB.

PRECEDENTS: There are many successful precedents of inter-governmental joint ventures or consortiums - among more than 7 states - to build and operate shared telecommunication or digital infrastructure, and not only standards, including:

- European Conference of Postal and Telecommunications Administrations (1959-, 48 states)
- Commonwealth Telecommunications Organisation (1979-, 52 countries)
- African Telecommunications Union (1995-, 55 countries)
- Asia-Pacific Telecommunity (1979-, 20 countries)
- International Mobile Satellite Organization (1982-, 150 countries)
- International Telecommunications Satellite Consortium, Intelsat (1964-, 200 countries)
- South American Telecommunications Network, SATNET (1988-, 8 countries)

Our initiative aims to realize a sort of “2.0, multi-governmental, mobile and ultra-secure” of the Minitel, the digital platform created by the French government in the 80’s, that became a bigger success than similar EU initiatives, constituting by 1988 a digital ecosystem with 3 million users of Minitel terminals, a dozen private and public compliant terminal makers, and thousands of private and public services and apps.

In a way, we are building a sort of "post-Cold War version of Crypto AG”, the de-facto global standard and state-of-the art for secret and diplomatic digital communications during the Cold War, that turned out to be controlled by only two states. As opposed to the original one, this new one is based on open democratic multilateralism, uncompromising transparency, and an ultra-resilient procedural front-door instead of technical back-door.

VISION 2030: Increasingly, with growing scale, TCCB-compliant mobile IT systems and mobile device will be made more powerful, secure, cheaper, and with more 3rd party apps, so as to be affordable to any ordinary citizen, and become their **personal trust hub and interface** to public e-services (e.g.EU eIDAS2), wearables, VR headset, and advanced AI services, and embedded in Kiosks in public offices and pharmacies. The certification body will gradually be extended to cover other critical societal systems, starting from social media feed systems, conversational AIs like ChatGPT, and beyond.

JOIN US: To learn more, contact us and join like-minded peers in **closed-door confidential** meetings at the 9th Edition of the Free and Safe in Cyberspace exploratory workshops, to be held (for the third time) in **Geneva next March 15-16th, 2023.**

A 30-page Executive Summary follows below detailing the benefits, the terms and conditions, a list of current public and private R&D partners, and a summary of the interest shown so far by multiple entities and ministries from over 9 states and IGOs, as you can read below in the *Traction* section. After NDA it is also possible to access a confidential 25-page *Detailed Traction Update* detailing of our engagements with those prospects.

Table of Contents

SUMMARY 3-PAGER **1**

OPPORTUNITY FOR STATES, IGOs and INGOs **7**

Summary of the Opportunity 7

The Spin-in Model: Relationship among TCA, TCCB and TRUSTLESS.AI 7

Detailed Description of Rights and Obligations 8

PROBLEM **10**

SOURCE OF THE PROBLEM **10**

SCALE OF THE PROBLEM **11**

PROPOSED SOLUTIONS: Why single states, the EU or the UN cannot solve it alone. **13**

SOLUTION: Trustless Computing Certification Body and Seevik Net **15**

Holistic Architecture: Ecosystem, Governance, Lawful Access 16

The Spin-in Model: a Uniquely Democratic Innovation Model 17

SECURITY APPROACH: Trustless Computing Paradigms **18**

Basic Principles Of “Trustless Computing” 18

KEY BENEFITS FOR COFOUNDER PARTNERS **20**

RELATIONSHIP TO OTHER INTERNATIONAL & EU STANDARDS **20**

TRACTION WITH NATIONS, IGOs & NGOs SO FAR **22**

Current Partners and Advisors 22

Prospective Partnership with States 23

Prospective Partnership with Inter-Governmental Organizations 23

Prospective Partnership with Global Cyber Powers 24

Prospective Partnership with State’s Strategic Investment Arms and IT Firms 24

More Details 25

PRIVATE MARKET DEMAND 25

SPECIAL BENEFITS FOR THE EU and/or EU STATES 25

SPECIAL BENEFITS FOR SMALL NATIONS 26

SPECIAL CASE FOR THE US, ISRAEL AND CHINA 26

NEXT STEPS & ROADMAP 29

JOIN US TO LEARN AND CO-DEVELOP THIS OPPORTUNITY 29

CONTACTS 30

MORE INFO & DOCUMENTS 30

OPPORTUNITY FOR STATES, IGOs and INGOs

Summary of the Opportunity

We are selecting **no more than 3 EU states, 4 globally-diverse non-EU states, 2 IGOs** (e.g., EU, UN agencies, Arab League) **and 2 neutral and fitting INGOs** (e.g. ICRC, Amnesty International) to become *cofounder partners* of the TCCB and Seevik Net initiative.

Cofounder partners will fund the entire initiative via an investment of €2 million each in order take **joint full inter-governmental control of the entire initiative**, including the TCA/TCCB, the startup spin-in TRUSTLESS.AI, the Seevik Net infrastructure, and several limited-time exclusive rights and privileges, while committing to later invite other states on an equal terms and with aim at maximizing global-diversity. INGO's and IGOs receive a 50% discount.

Cofounder state, IGO and INGOs *partners* will enjoy temporary special privileges, including: (1) receive 900 device units each; (2) be able to establish TCCB-compliant hosting rooms; (3) participating with their firms to the development rather than just oversight of Seevik Net; (4) participating in the initial TCB governance that will give shape to its statute and first operational version of the *Trustless Computing Paradigms*; (5) private and public entities headquartered in their territory will have exclusive access for the first 12 months (5.a) to purchase a TCCB-compliant IT system and (5.b) to submit IT services for certification from TCCB.

The full cost of the initiative is about **$18 million**, includes: making the TCCB operational; finalization, testing and production of Seevik Net, including 15,000 units of TCCB-compliant mobile client devices (in *Seevik Wallet* or *Seevik Phone* form factors); the creation of one TCCB-compliant data room, realized in prefabricated and containerized units. Having a TCCB hosting room in their territory/premises is optional for co-founder *partners*, so its the costs are borne by each that chooses to have one, except for assistance in localization, integration and customization for compliance to local laws and desiderata while remaining TCCB-compliant.

We are also selecting no more than 5 states will be selected as *non-founder state governance partners*, at the cost of $**20 thousands** with full right to participate in the TCCB governance, but none of the other rights lesser rights and privileges. Up to 3 states will be selected as free-of-charge *observer state partners* at the cost of **$10 thousands** per year.

The Spin-in Model: Relationship among TCA, TCCB and TRUSTLESS.AI

The Trustless Computing Association has been building the TCCB. It is currently controlled by TCA founder and Exec. Director Rufo Guerreschi, a person of his trust, and TCA deputy director Nick Kelly. Once 7 states have joined as *co-founder partners*, TCA will rename itself into TCCB, and enact the **permanent inter-governmental democratic governance**, as specified in its statute (and follogin revisions).

TRUSTLESS.AI, its startup spin-in, has been building Seevik Net. Once TCA/TCCB has moved to its permanent governance it acquires an option to buy 100% of the spin-in shares at the price of $20 million, as specified in *spin-in* agreement among the two organizations. This spin-in model has enabled the leveraging of private sector innovation, while **ensuring a highly democratic multi-national long-term control** (see precedents in the German DoD BWI project).

All shares and shares rights holders of the spin-in will be "bought out" all at once for €6 million, via funds that will be contributed by the next 3 states that will join as *founding state partners,* so as to **remove any long term private influence**, and give completion to the spin-in model. (While spin-in CEO Rufo Guerreschi has contributed over $350K and 6 unpaid man-years, and owns 100% of the shares, a number of angel investors, his cofounder, advisors and team members have invested several man-years and over $250k, and so have accrued about 35% of the share rights.)

Detailed Description of Rights and Obligations

Each *Cofounder Partner* state, IGOs and INGOs (when it applies) will be subject to these rights and obligations:

1) **Acquire full joint control of TCA, TCCB, the startup spin-in and Seevik Net**
    a) Acquire 5.6% of voting power in the TCA/TCCB Assembly, which will amount collectively to 51%. Such collective voting rights share will be reduced to 30% as foreseen decision making entities will be activated.
    b) Acquire 5,6% of the shares of the startup spin-in and 11.1% of the voting rights, which will amount collectively to 51% of shares, and 100% of the share voting rights.

2) **Receive 900 TCCB-compliant mobile client device units**;
    a) Acquisition of 900 user-seats and client units of Seevik Net (either Seevik Wallet or Seevik Phone) for officials of their organizations, plus a 30% discount on up to 1800 additional units for close personal or professional associates;

3) **Participate early in TCCB governance to shape statute and *Trustless Computing Paradigms***;

4) **Local firms can purchase, resale and certify TCCB systems, exclusively for 1 year;**
    a) local private and state cybersecurity startups, VCs, IT firms, defense firms, will be able to build and certify compliant systems and sell them abroad, with major

economic development.

5) **Participate via local to the paid development of Seevik Net**;
    a) Right for their strategic tech firms specialized in high-assurance low-level open IT to participate and be paid for in the consortium building Seevik. the architecture, development, and/or oversight of both TCCB and Seevik Net so as to increase their confidence in the outcomes, and position their firms to benefit economically in the TCCB ecosystem.
    b) Right to participate as strategic investors **-** via their state-controlled cybersecurity funding or VC entities - in the startup spin-in of TCCB, TRUSTLESS.AI with other founders. As per a spin-in agreement, the startup is bound to accept acquisition offers by the TCCB at precisely-set non-speculative prices.

6) **Receive the right and full assistance to establish local TCCB-compliant hosting rooms**;
    a) Acquire the right to host one or more state TCCB hosting rooms on their territory, or in their headquarters for IGOs and INGOs with international immunity like ICRC, UN and EU.
    b) Such a hosting room will host an encrypted copy of all communications of users that are their citizens or foreign users using TCCB client devices in their territory. Exception to the above will be communications that involve foreign users physically located outside their territory which will instead be stored either in (i) another partner states' TCCB hosting rooms or (ii) in a set of 3 TCCB-managed TCCB hosting rooms located in 3 neutral globally-diverse states, whose lawful access requires the request to be approved by the TCCB judicial Board.
    c) Such state TCCB hosting rooms will be set up and managed in compliance with the TCCB Cloud which includes the physical in-person approval of all lawful access requests by a jury-like group of five random-sampled citizens, according to local laws.

7) **Enjoy special publicity and event-hosting rights**.
    a) Such rights will apply to TCCB and Seevik Net main documents, communications and events, and include the right to submit their candidacy to host a future edition of the Free and Safe in Cyberspace conference series.

8) **Commit to actively participate in good faith in the decision making of the TCCB organs**;

9) **Commit to share with TCCB any vulnerabilities found TCCB-compliant systems**;
    a) Commit to exert their "best effort" to ensure that all governmental and private firms agencies based in their territory will share with TCCB, and only with TCCB, any information the come in possession about actual or potential technical or

organizational vulnerabilities in TCCB-certified IT, or TCCB organs or organizational infrastructure as well as tools and methods to exploit such vulnerabilities, and evidence of crimes by or against any members of the TCCB organs. Sustained and grave failures in such efforts, regardless of maliciousness, can result in suspension or revocation of TCCB partner status.

PROBLEM

In early November, it was revealed that the then foreign minister of the UK, Liz Truss, was spied on for months on her communications with colleagues, friends and foreign diplomats.

A few days later, Ignazio Cassis, the president and foreign minister of Switzerland, the political editor of the BBC, and 100 other personalities, were revealed to have been victims of *hacking-for-hire* by Indian hacker gangs, via UK legal firms, via unknowns.

They are in good company. Last year alone, the sitting **prime ministers** of Spain and of Finland, the son of the new prime minister of Israel, the head of opposition of Greece and of Poland, in what the Rapporteur of the EU Parliament 48-strong Committee on Spyware referred to as ***"much, much worse than Watergate".***

Same fate was suffered by the editor of the Financial Times, who suffered similar total unchecked spying. And that's just the hacks that were discovered and disclosed by the victims! Even the president of the US runs the same risks, as detailed in 2017 by the New York Times.

Such spyware are undetectable, often leave no trace, take full control of the device, by being able to read all information, and turn on the microphone at will. Not only they are spied on and blackmailed, but state and non-state hackers, domestic and foreign, but in an attempt to reduce their risk they are forced to renounce to communications and self-censor themselves, causing huge inefficiencies in their professional and private lives.

SOURCE OF THE PROBLEM

Are hackers just too good? Can't those phones be made more secure?

If you are to believe mainstream media, the reason why any and all client device available on the open commercial market, including the iPhone - even with the best protection software and hardware, and managed in the most careful ways - remain so incredibly vulnerable to so many actors has to do with the fact that while companies like Apple do their best, state and non-state hackers becoming are beating them at the security game.

But every year, Apple, top Android phone makers, and cybersecurity protection suite makers, introduce new security improvements. Like a mirage, decent security is never attained.

Why is that? Sure, state and non-state hackers keep significantly increasing their investments. Yet, we can make IT devices that are both reliably secure against the most advanced attackers and accessible to interception only to intended entities - as argued in this detailed academic paper by the Trustless Computing Association, and as shown in practice by Crypto AG, the Swiss-based western standard devices for secure diplomatic communications in the Cold War.

Two are the real root causes. First, hyper-complexity and obscurity are demanded by competition for rich entertainment performance features that are required of top-end smartphones. Second, the unconfessed need to surreptitiously ensure that several powerful states can hack them at any time to prevent terrorist, enemy or adversary states.

In addition, carrying an **extra device** may be acceptable for the most targeted persons but too cumbersome for their many sensitive non-classified interlocutors.

Even the best secure messaging apps **cannot be more secure than the device** they run on, while **all smartphones and IT standards and certifications are hyper-complex** and **systematically and surreptitiously weakened by powerful states** to retain their capability to pursue criminals and adversary states, as we've learned from Snowden onwards.

Even worse, these structural processes' **surreptitious nature** and "plausible deniability" causes innumerable other entities to discover, buy, steal, or just rent access to those hacking capabilities.

SCALE OF THE PROBLEM

The number of those hacked or at risk is not easy to quantify or even approximate, by design. Security agencies go to great lengths to **ensure that a large number of criminals and terrorists over-estimate the security of secure mobile solutions** so that they can continue their legitimate interception, while spyware and secure IT companies like Apple play along, for profit reasons.

But once in a while, some hard verified data comes around. The lawsuit that Facebook has against NSO Group provides details and proofs of 1400 WhatsApp hacked worldwide in the course of just 2 weeks. The NSO Group, just one of a dozen spyware firms in Israel alone, testified last June to the 42-strong EU Parliament Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware that over 12,000 citizens each year are hacked via their Pegasus system.

But those numbers (1) do not include dozens of other similar spyware companies that rent or sell to states and private groups; (2) nor do they include those hacked by security agencies of powerful states like the US, China and Russia; (3) nor hundreds or thousands of other entities to **discover, buy, steal, or just rent access to illegitimately hacking of high-profile users**, as shown by Shadow Brokers and Vault 7 scandals, as consequence of the surreptitious way in which powerful states ensure their "backdoor" access.

Last October Kaspersky declared it had found and "fully deconstructed" the most advanced German and UK spyware, FinFisher, enabling them to fully re-use it. The same could have been done by others. Already ten years ago powerful state security agencies like, and to a lesser extent some semi-private spyware companies, had capabilities to turn targeted surveillance into a scalable enterprise via systems and programs like the NSA FoxAcid and NSA Turbine.

Furthermore, a vast majority of these cyber crimes go **undiscovered** for years, if ever, as they often leave no trace, as outlined above. When discovered, they are nearly always kept secret as both victims and attackers gain from keeping them **unreported**. Victims are not required to disclose. Hacking of state officials is often classified as **state secret**.

Apple declared in 2021 that the attacks should not worry because exploits: "*cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals. While that means they are not a threat to the overwhelming majority of our users,the overwhelming majority of our users*". Their use of the term "overwhelming" is compatible with hundreds of thousands of devices hacked, which would amount to 0.01% of the 1.5 billion iPhones out there.

The New York Times reported in 2018 about NSO Group: "*Clients could then pay more to target additional users, saving as they spy with bulk discounts: $800,000 for an additional 100 phones.*", which brings the price to €8,000 per target (Though the price is apparently higher nowadays). And that's for the Rolls-Royce of hacking tools!

From the above, we can therefore estimate that **the number of victims are in the many hundreds of thousands** every year, while **those at risk are in several millions** world-wide.

As opposed to what security agencies, smartphone makers and uncritical media want us to believe **those most at risk have known the truth for some time now**. Pre-Covid surveys by UBS and by Northern Trust showed that the **16 million wealthiest persons in the World and family offices regard cybersecurity as their n.2 or their n.1 concern**, respectively. There is nothing money can buy.

Paradoxically, on the other hand, legitimately authorized judiciary of democratic states are often unable to enforce legal intercept orders on such smartphone - as it happened with the deleted encrypted messages of US president's secret service detail on Jan 6th 2021 and leaders of a top swiss private bank - because the best spyware is unavailable to them, or is limited in use forstate security cases - while criminals may have acquired such evidence before its deletion for use in blackmail.

It is nothing short of a **public security and democratic emergency,** as well as a huge market demand.

PROPOSED SOLUTIONS: Why single states, the EU or the UN cannot solve it alone.

More than any other governmental institution around the World, the EU is attempting to solve this huge problem by **regulating spyware** and **setting requirements and certification for more secure mobile devices**. Yet, the current approaches and EU's own institutional constraints make it very unlikely it'll be able to truly tackle this problem. A recent draft report by the EU Parliament PEGA Committee on Spyware, in line with recommendations by leading human rights NGOs, calls for urgent national and EU **regulation of spyware**.

This is needed and useful, but will inevitably have very limited effect. Due to the huge technical, operational and jurisdictional complexities of spyware - and the hyper-complexity and chronic vulnerability of even the most secure smartphones - such regulations (a) would be very hard to enforce, (b) attribution of hacks would remain extremely difficult, and (c) law-abiding officials and citizens would anyhow remain hackable by innumerable entities located outside the regulators' jurisdiction, while law enforcement and intelligence would loose a critical tool to fight crimes and terrorists.

The recently announced EU Cyber Resilience Act is not going to even remotely protect millions of highly targeted individuals because:

1) It does not require full **transparency** of source designs, and **extreme levels of security review in relation to complexity** of all critical processes, even down to chip fabrication oversight ("security is the weakest link"!)
2) It does not face the "elephant in the room", i.e. the needs of **legitimate lawful access**, by having a transparent international "in-person" procedural mechanism to manage requests by security agencies,state, EU, allied and beyond.
3) High and ultra-high levels of assurance **cannot be certified ex-post**, i.e. without assessing all assess technology, process and persons critically-involved **ex-ante** in the supply chain and lifecycle, so as to estimate the probability of undetected willful or accidental vulnerabilities - as well as the training and incentive placed on end-users.

In addition, the EU Council has already suggested changes to enable EU states to make devices that are too secure illegal on "national security" grounds. The *EU Media Freedom Act* that is also not remotely going to protect journalists in the EU as pointed out recently by the EDPS.

Hopefully, EU member states and parliamentarians will succeed in amending the Cyber Resilience Act to add much more stringent security **requirements for the most vulnerable users**, in a mandatory or voluntary way. But unfortunately, the EU unanimity decision-making, combined with the lobbying power of Big Tech and powerful states, will likely obstruct such efforts, as we've seen before for privacy Acts.

Since, as discussed above, states, the EU and the UN cannot solve this problem, we propose - as a fail-safe initiative to be brought forward concurrently with policy efforts within those institutions - that some EU member states, parties and parliamentarians - while trying to get the needed amendments approved - move ahead together with non-EU globally-diverse like-minded to **build and govern the certifications and compliant IT that are needed** to shape a fair, safe, effective and participatory global digital sphere for elected officials, diplomats and all citizens.

OUR SOLUTION: Trustless Computing Certification Body and Seevik Net

This section assumes you have read the 3-page Summary at the start of the document.

Last June 2021, in Geneva, we established the *Trustless Computing Certification Body,* **a new inter-governmental democratic IT security certification body** to guarantee both radically-unprecedented security and privacy as well as "in-person" procedural *legitimate* lawful access for sensitive yet non-classified communications.

Concurrently, via its startup spin-in, TRUSTLESS.AI, since 2019, we are building an initial TCCB-complaint private cloud, mainstream mobile app and **2mm-thin mobile device** - embedded in custom leather wallets (video animation) or in the back of Android smartphone (video of the Seevik Phone Proof-of-concept device) - that aims to far outcompete in both security, convenience and accountability even the best-protected iPhones and the best commercial *cryptophones*.

We achieve radically-unprecedented levels of trustworthiness by (A) applying to both **extreme, battle-tested, and open** (technical and organizational) **socio-technical safeguards, and checks and balances** - the Trustless Computing Paradigms - that are applied to all technologies and processes critically involved in the entire life-cycle - down to fabrication oversight, CPU design and hosting room access and via (B) a governance model and statute that highly maximizes global **democratic accountability**, socio-technical competency, and resiliency from state pressures.

The initial version of Seevik Net will derive from the **hardening and integration of battle-tested open-source IT** stacks, via a resilient consortium of carefully-vetted technical partners in suitable states, which will include (a) seamlessly **portable 2mm-thin client devices**, carried in custom leather wallets (video) or embedded in the back of smartphones (video), with special 3rd party apps; (b) **interoperable messaging and social apps** for mainstream stores, (c) a **custom private cloud**, made up of decentralized nodes running on TCCB client devices, and multi-national network of hosting rooms according to our TCCB Cloud process.

TCCB Cloud process requires that all sensitive data and code is stored in **4 TCCB hosting rooms in states part of at least two different military/intelligence alliances**, and approval by a ***TCCB Jury* of 5 random-sampled citizens** - for a local lawful access request - and by such jury executing decision by an international ***TCCB Judicial Board*** - for international ones. The initiative will eventually be opened for joining by all states on a fair and equal basis.

TCCB is a new standards-setting and certification body that will certify IT services for human communications aimed to ensure both (1) **radically-unprecedented levels of confidentiality, integrity and democratic control** and concurrently (2) safe "in person" international ***legitimate***

lawful access mechanism. Meanwhile, via our *spin-in* we are building an initial set of IT systems - minimal but complete and mandatorily interoperable - that will constitute **Seevik Net**, a global democratic human computing sphere and platform, alongside existing dominant platforms.

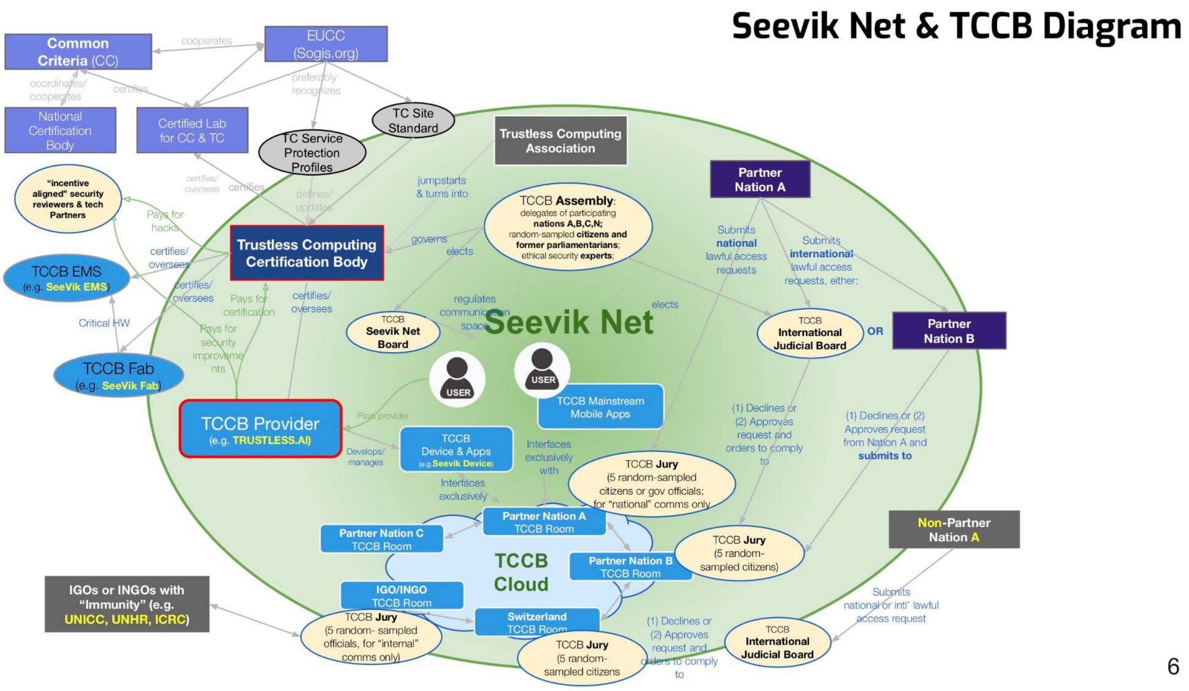
TCCB aims to create and regulate a **new global democratic digital public sphere** - with apps, cloud, and devices, that run parallel to mainstream ones and over the open Internet. TCCB and Seevik Net will **radically increase** citizens' **privacy, security, and democratic control** of their sensitive digital lives; **defend democratic institutions** from the rise of authoritarianism, at home and abroad, inside and outside institutions; and **foster fair and effective dialogue and understanding, within and across states**.

Holistic Architecture: Ecosystem, Governance, Lawful Access

The initial version of Seevik Net will derive from the **hardening and integration of battle-tested open-source IT stacks**, via a resilient consortium of carefully-vetted technical partners in suitable states, which will include:

- (a) seamlessly **portable 2mm-thin client devices**, carried in custom leather wallets (video) or embedded in the back of smartphones (video), with special 3rd party apps;
- (b) **interoperable messaging and social apps for mainstream stores**;
- (c) a custom private cloud, made up of decentralized nodes running on TCCB client devices, and a multi-national network of hosting rooms according to our TCCB Cloud process.

TCCB Cloud process requires that all sensitive data and code is stored in **at least 4 TCCB hosting rooms in states part of at least two different military/intelligence alliances**, and approval by a TCCB **Jury of 5 random-sampled citizens** of the host state- for a state lawful access request - and by such jury executing decision by an international ***TCCB Judicial Board*** - for international lawful access requests.



Seevik Net & TCCB Diagram

Common Criteria (CC)
cooperates
EUCC (Sogis.org)
coordinates/ cooperates
certifies
preferably recognizes
National Certification Body
Certified Lab for CC & TC
TC Site Standard
TC Service Protection Profiles
Trustless Computing Association
"incentive aligned" security reviewers & tech Partners
certifies/ oversees
certifies
defines/ updates
jumpstarts & turns into
Pays for hacks
certifies/ oversees
Trustless Computing Certification Body
governs
elects
TCCB Assembly: delegates of participating nations A,B,C,N; random-sampled citizens and former parliamentarians; ethical security experts;
Partner Nation A
Submits national lawful access requests
Submits international lawful access requests, either:
TCCB EMS (e.g. SeeVik EMS)
certifies/ oversees
Pays for certification
certifies/ oversees
regulates communication space
Seevik Net
elects
TCCB Seevik Net Board
TCCB International Judicial Board
OR
Partner Nation B
Critical HW
Pays for security improvements
TCCB Fab (e.g. SeeVik Fab)
USER
USER
TCCB Mainstream Mobile Apps
Pays provider
TCCB Provider (e.g. TRUSTLESS.AI)
Develops/ manages
TCCB Device & Apps (e.g.Seevik Device)
Interfaces exclusively with
(1) Declines or (2) Approves request and orders to comply to
(1) Declines or (2) Approves request from Nation A and submits to
TCCB Jury (5 random-sampled citizens or gov officials; for "national" comms only
Interfaces exclusively
Partner Nation A TCCB Room
Partner Nation C TCCB Room
TCCB Cloud
Partner Nation B TCCB Room
TCCB Jury (5 random-sampled citizens)
Non-Partner Nation A
IGOs or INGOs with "Immunity" (e.g. UNICC, UNHR, ICRC)
IGO/INGO TCCB Room
TCCB Jury (5 random- sampled officials, for "internal" comms only)
Switzerland TCCB Room
TCCB Jury (5 random- sampled citizens
(1) Declines or (2) Approves request and orders to comply to
TCCB International Judicial Board
Submits national or intl' lawful access request
6

The Spin-in Model: a Uniquely Democratic Innovation Model

An initial set of open-licensed TCCB-compliant systems, devices and services, Seevik Net, is being built through the startup "spin-in" TRUSTLESS.AI that the Trustless Computing Association, created in 2019. According to the spin-in model, a signed agreement ensures that the **startup spin-in TRUSTLESS.AI and Seevik Net will be mandatorily owned and controlled by the TCCB** - via an option by TCCB to buy 100% of its shares at precisely-set non-speculative conditions - to leverage private sector innovation while ensuring a highly democratic and multi-national long-term control of such a sensitive transnational democratic infrastructure, such as the BWI project of the German defense ministry, but multi-national.

SECURITY APPROACH: the Trustless Computing Paradigms

TCCB and Seevik Net will achieve radically-unprecedented levels of trustworthiness by (A) applying to both **extreme, battle-ftested, and open** (technical and organizational) **socio-technical safeguards, and checks and balances,** the Trustless Computing Paradigms, that are applied to all technologies and processes critically involved in the entire life-cycle - down to fabrication oversight, CPU design and hosting room access and via (B) a governance model and statute that highly maximizes global **democratic accountability**, socio-technical competency, and resiliency from state pressures.

The Trustless Computing Paradigms describes a novel IT security approach - and a new IT security certification model for IT systems to be labeled "Trustless Computing" - that is centered on (a) **uncompromising transparency** of source designs and **extreme security-review in relation to complexity of all critical components and processes in the entire lifecycle**, and on (b) **democratic, time-tested, and decentralized governance, certification and oversight processes**.

Basic Principles Of "Trustless Computing"

- *Trustless Computing* is a novel approach to IT security and the name of an IT system certified by the Trustless Computing Certification Body that aims and claims to achieve **radically-unprecedented levels of confidentiality and integrity for sensitive human computing and communication** while ensuring **improved "in-person" national and international *legitimate* lawful access**, without requiring any legislative changes anywhere.

- *Trustless Computing* can be conceived as an extreme uncompromising version of the security-by-design approach to IT security, which expands "security design" and early-on deep verification to all critical technologies, supply chain processes and organizational processes critically-involved.

- *Trustless Computing* is centered on (a) **transparency of source designs** and **extreme security-review in relation to complexity** of all critical components and processes in the entire lifecycle, and on (b) **democratic, time-tested, and decentralized governance,** certification and oversight processes.

- *Trustless Computing* is a novel approach to IT security whereby actual and perceived confidentiality and integrity for an IT systems, service and experience - just as that of **electoral processes** in a resilient mature democracies - is not a technical problem but ultimately 100% the **by-product of the accountability and transparency of the design of the organizations and human processes** critically-involved in the entire lifecycle, as can be assessed by moderately educated and informed citizens.

- *Trustless Computing* **renounces the need or assumption of any upfront unverified trust** in any organization, technology and person. *Trustless Computing* is not based on **distributed ledger technologies or blockchain** systems, while it may include them. Trustless Computing is different from **zero trust**, while it fully embeds its principles. Trustless Computing can be construed as an extreme deeper version of the **security-by-design.**

- Trustless Computing acknowledges that if only one our 16 million commercial airliner fights results in an accident, whereby every smartphone produced is hacked but a innumerable entities, it is not due to the fact that IT is harder, but **because all IT and IT standards are structurally weakened and surreptitiously compromised by nations** due to their failure to reconcile the needs of personal privacy with that of national security. Just as leaving "keys under a doormat", bug-doors are and will always be in all systems until a new mechanism ensures both the utmost system security and privacy and a safe-enough front-door access.

- *Trustless Computing* fully includes and embeds in its paradigms and certification processes the **zero trust** approach to IT security, yet it extend its "*never trust, always verify*" concept and an extreme "security-by-design" approach to the (a) technical and organizational "checkpoint" components that exercise Zero Trust functions in the Zero Trust architecture applied to the target system; as well as (b) the underlying target system in their entire supply chain and lifecycle. (See more in this recent post).

- *Trustless Computing* is **not** an IT security approach based on the **distributed ledger technologies or blockchain system or standard**, while a Trustless Computing IT system that satis it may include them. Many in its ecosystem have referred to their domain or specific solutions as "trustless systems". We challenge the claims that DLT/blockchains constitute a "trustless" system as well as a *standalone* trustworthy system because it requires the user - in varying degrees - to **blindly trust** (a) that several key actors in the power structure of a given blockchain will not act maliciously or collude to do so; (b) their hardware "crypto" wallet for integrity, and their software wallets and clients device for integrity and confidentiality. Conceptually, their flaw comes from thinking that digital **decentralization that is not democratically governed** and a server-side infrastructure without client devices, can alone deliver trustworthiness of sensitive IT systems beyond a digital speculation mechanism, like Bitcoin.

KEY BENEFITS FOR COFOUNDER PARTNERS

Firstly, the participant state would radically increase both (A) the **protection of legal communications** and (B) the **accountability of illegal communications** for its most sensitive law-abiding citizens and organizations, including elected officials, journalists, business leaders, activists, as well as their reference organizations.

It will radically increase protection from politically-motivated extortion, blackmail, manipulation, or profit-motivated extortion, ransomware and trade secret spying.

Secondly, the participant state would **increase the certainty, integrity, and attribution capability of your security agencies' when investigating users of TCCB-compliant systems, foreign and domestic, as opposed to other IT systems**.

In fact, while their security agencies would "by definition" lose the arbitrary capability to hack into TCCB-compliant systems (which will be designed with the stated purpose of being impregnable to such acts) - when legitimately authorized - they will: (A) have higher assurance of prompt access, without the risk of "going dark" or being unable to hack, and independently from the availability to assist of other states or firms; and (B) obtain more solid and forensic-friendly evidence that is much more reliable, and that will be accepted by the highest state courts, unlike that obtained via targeted hacking which does not stand in the highest courts in Germany and France.

Thirdly, the participant state would **be recognized by other states as a leader in promoting peace and fair and effective global cooperation** by participating in building nothing less that a post-Cold War version of Crypto AG, the de-facto global state-of-the art for sensitive and diplomatic digital communications during the Cold War, that turned out to be controlled by only two states.

As opposed to the original one, it is based on open democratic **multilateralism**, uncompromising **transparency**, and an ultra-resilient **procedural front-door** instead of a technical back-door - and available to all in a highly convenient way. Beyond diplomats, it'll be available to millions of targeted law-abiding persons and organizations with portability and convenience via 2mm-thin standalone devices, carried inside custom leather wallets or in the back of future smartphones, and then other form factors.

RELATIONSHIP TO OTHER INTERNATIONAL & EU STANDARDS

TCCB will certify systems that at once comply with the highest assurance levels of the EU digital identity and transaction standard, **eIDAS 2.0 High**, while offering levels of confidentiality and integrity of human computing radically beyond state-of-the-art. TCCB will start as a high-level but binding certification framework, and quickly move towards a thoroughly detailed certification scheme akin to **Common Criteria**.

While free-standing as an inter-governmental initiative for voluntary certifications, TCCB will be complementary, synergistic, and inspirational for existing, upcoming and future EU and UN promoted cybersecurity certifications.

To that end, it will also be proposed as a “schema” within the **EU Cybersecurity Certification Framework** and as a new initiative under **UN International Telecommunication Union** (ITU-T) processes. It will also promote future downward compatibility in respect to EU Secret and **Common Criteria EAL4-6** for future use in advanced governmental sectors.

Initial TCCB target domain will be that of human transactions and communications that are non-classified from sensitive to ultra-high requirements of confidentiality and integrity. Initially, the target users of TCCB-compliant IT services will be millions of law-abiding highly-targeted and politically-exposed persons and organizations, such as investigative journalists and news organizations, politicians and political parties, private banks, family offices, exposed enterprises, and NGOs. At a later stage, it will expand to use cases requiring also *high* and *ultra-high availability*, including critical governmental communications, AI, and cyber-physical systems.

TRACTION WITH NATIONS, IGOs & NGOs SO FAR

Over recent years, months and weeks, we received substantial interest from several states, including **Germany, France, Italy and the Netherlands** - but also the US and Israel, and some smaller third states with high strategic autonomy like **Switzerland, Malta and Liechtenstein**. Such interest includes dozens of hours of engagements by relevant high-level current and former government representatives (foreign affairs, security agency, minister level, parliamentarians), and by suitable low-level tech firms from the same states, and many dozens of hours of engagements with **six state-close/controlled cyber-only venture capital firms** interested to co-invest with other private and public counterparts in the startup-spin-in.

We held over nine meetings with **former highest-ranking cyber diplomats of the US and Israel**, following which we wrote an all-important detailed case as to why Israel and the US should and will eventually join as governance partners of the Trustless Computing Certification Body - even though they'd need approval by an UN-like resilient, democratic body to intercept an elected official or private citizen from a friendly nation. MACH37, the McLean-based **United States** leading cybersecurity accelerator, chose us among hundreds of candidates for their program in Q4 2021 and accrued rights to 3% of the start spin-in shares. (In early October, the Agenzia Della Cybersicurezza Nazionale of Italy announced investments in strategic cybersecurity startups).

We have engaged with some interest with several top executives of **Huawei** global and Swiss in 2019-2020, as one of two smartphone partners (one western and one non-western) for building initial mobile device and system complaint to the TCCB Seevik Phone, and as a proxy for engaging with the **Chinese government**. We made some attempts to engage China, over the years, without success. But last November, we initially engaged **a *Secretary of the China Mission to the UN in Geneva*,** in charge of activities at the UN ITU for IT standards, and we are looking forward to a 1 to 1 or joint meeting soon.

For more information, we have available on qualified request a **Detailed Traction PDF, a 25-pager deck PDF profiling our current R&D and governance partners** of TCA, TCCB and Seevik Net, as well as the extensive interest shown so far by several countries - through their relevant ministry, strategic IT security companies, and cyber-only funding vehicles - with a 2-pager summary on top.

Last June 2021, the 8th Edition of our Free and Safe in Cyberspace conference held last June 2021 in **Geneva**/hybrid - after previous editions in Brussels, Berlin, New York, Geneva and Zurich - we finalized the Trustless Computing Paradigms, and the statute of the *Trustless Computing Certification Body* ("TCCB") - together with World-class speakers, including top IT security experts, the former top cyber diplomats of USA and Netherlands, and executives of top EU banks.

Current Partners and Advisors

Since 2015, we have advanced TCCB and Seevik Net via R&D initiatives and academic papers, together with 35 top R&D partners and 25 top advisors, and a global conference series called **Free and Safe in Cyberspace** with 8 editions held on 3 continents, with over 120 exceptional speakers. In 2019, we created a *spin-in* startup, TRUSTLESS.AI, with a top team, advisors, and investors, building initial minimalist TCCB-compliant IT systems - which is bound to be re-owned by TCCB via a "spin-in" agreement.

Together with global tech leaders in high-assurance open-source low-level IT and ***EOS*** (EU largest IT security industry association), the national IT certification bodies for top secret IT of **Austria** (A-SIT, CIO) and **Italy** (ISTICOM/OCSI), equivalents of the German BSI, have been among our formal governance R&D partners in our 2015-2016 EU funding proposals for TCCB and Seevik Net, to radically improve the transparency, the security levels and the mutual recognition of classified IT certifications.

Prospective Partnership with States

While no written agreement is in place yet - except R&D ones with Italy and Austria - over recent years, months and weeks, we have attracted the substantial interest of several nations via engagement with top representatives of different relevant departments and ministries, their strategic cyber-only investment entities, or their strategic low-level IT security firms. For each, we have engaged one or more of the following (1) their foreign affairs, security, intelligence, or IT certification departments for participation as **governance** partners in TCCB; (2) their state-funded or state-controlled VCs or **funding** entities specialized in strategic investments in IT security for joint controlling investment in our startup spin-in; (3) their strategic IT security firms specialized on high-assurance open-source low-level IT for **technical partnership**, primarily based on a few open-source derivative designs of the open-source **Sel4** operating system and the open-source **Risc-V** CPU/SoC designs.

Over the last 5 years, very extensive engagements have occurred with **Germany** and **Italy** at all levels. More recently, with **France**, **Netherlands,** and several third nations with high strategic autonomy like **Switzerland, Malta, Qatar**, and **Liechtenstein**. Some interest has been shown by **Romania** and **Poland**. In recent months, following meetings in DC, London, Munich, and Vaduz, we have presented a customized presentation of the opportunity for Germany, and for Liechtenstein and for Middle East nations. Details of those engagements are available on request. in a 25 pager document.

Prospective Partnership with Inter-Governmental Organizations

While no written agreement is in place yet, on the front of IGOs (Inter-governmental Organizations) interested in joining, we recently received substantial top-level interest from UN International

Computing Center to develop the TCCB and Seevik Net inside the **United Nations** as per this proposal for the United Nations, via a new "voluntary fund" which is being set up for critical UN IT needs. In recent weeks, we have had increasing interest in several meetings with the **International Committee of the Red Cross.**

Prospective Partnership with Global Cyber Powers

Initial participation by **global cyber superpowers**, like the US, China and Israel would be welcome but not required, and incentivized via higher temporary influence for those that join earlier rather than later.

While no written agreement is in place yet, over the last two years, we held over nine meetings of intense and detailed dialogue with the former highest-ranking cyber diplomats of both the **US and Israel.** Following such dialogues, we wrote an all-important detailed case as to why **Israel** and the **US** should and will eventually join as governance partners of the Trustless Computing Certification Body - even though they'd need approval by an UN-like resilient, democratic body to intercept an elected official or private citizen from a friendly nation. MACH37, the Virginia-based US leading cybersecurity accelerator, for which we were chosen among hundreds in Q4 2021, has accrued rights to 3% of the shares of the spin-in TRUSTLESS.AI.

When and if the US and/Israel will decide to participate, we believe it would be crucial that China participated as well because it would make TCCB, Seevik Net and TCCB-compliant IT (1) more equally trusted worldwide, to **enable the fair and effective global dialogue,** at all levels, to promote **peace and joint tackling of global challenges;** and (2) substantially **more trusted even by western citizens, elected officials, diplomats**, and even prime ministers, given the experience of programs like Crypto AG, NSO Group, the iPhone, and past overreach of western security agencies.

We made some attempts to engage China, over the years, without success. Last November, we initially engaged a **Secretary of the China Mission to the UN in Geneva**, in charge of IT standards at the UN, and we are looking forward to a 1 to 1 or joint meeting soon. We have engaged with some interest with several top executives of **Huawei** global and Swiss in 2019-2020, as one of two smartphone partners (one western and one non-western) for the Seevik Phone, and a proxy for engaging with the Chinese government.

Prospective Partnership with State's Strategic Investment Arms and IT Firms

While no written agreement is in place yet, in recent years and months, we had dozens of meetings for over 30 hours with **cyber-only state-funded or state-controlled VC firms** to jointly invest in the association *spin-in* startup TRUSTLESS.AI, which is building initial TCCB-complaint IT systems and will provide initial funding for the TCCB. And maintain active interest with some from **Germany** (eCapital Entrepreneurial Partners), from **Netherlands** (Innovation Quarters), **France** (Cyber Impact Ventures), and the **USA** (Paladin Capital Group). (In October 2022, **Italy** announced a program to invest in strategic cybersecurity startups). MACH37, the US leading cybersecurity startup accelerator, in Washington DC, for which we were chosen among hundreds in Q4 2021, has accrued rights to 3% of the share rights (not yet the shares). We are actively seeking for a similar participation by a **Chinese** entity to counterbalance such participation.

In recent months, we've been engaging intensely with (global and national strategic) tech firms specialized in the co-development of **multi-national open-source high-assurance battle-tested CPUs and OSs**, from the same countries, based on **Risc-V** and **Sel4**. These include especially *Hensoldt Cyber* (**Germany**, but indirectly invested by **Italy** and **France**), but also Galois Inc. (**US**), Technolution (**Netherlands**) and the global **Sel4 Foundation**, for their participation as technical partners. These will make it so that participating nations - and all nations and the general public - will have full and transparent access to the TCCB standards, initial complaint IT and its architecture, throughout its lifecycle, from its inception, maximizing actual and perceived trust in the resulting tech by nations and all citizens. Seeking further engagement with strategic firms from **China** and non-aligned countries.

More Details on Prospective Partner

Available after qualified request, and a signed NDA or signed Terms of Participation agreement: a *Detailed Traction Update*, a 25-pager deck PDF profiling our current R&D and governance partners of TCA, TCCB and Seevik Net, as well as the extensive interest shown so far by several countries - through their relevant ministry, strategic IT security companies, and cyber-only funding vehicles - with a 2-pager summary on top.

PRIVATE MARKET DEMAND

Private market demand is very significant. Pre-Covid surveys by UBS and by Northern Trust show that even the 16 million wealthiest persons in the World and family offices regard **cybersecurity as their n.2 or their n.1 concern**, respectively. There is nothing money can buy. Even the richest have nowhere to hide, not to mention journalists, executives and activists.

Participating states could promote significant economic development by acquiring a limited-exclusivity for their firms and financial institutions in offering TCCB-complaint systems. Several banking and SME associations have shown initial interest in TCCB and Seevik Net for their members and for their members' clients.

SPECIAL BENEFITS FOR THE EU and/or EU STATES

Our TCCB is meant to inspire amendments or extensions to new regulations that have been proposed to regulate spyware and to created certifications to ensure much more secure devices - in the EU, EU states and around the World - and **fill the gap** in the meantime, while planning to be “downward compatible” with them.

Our initiative aims to complement the *EU Cyber Resilience Act* and *EU Media Freedom Acts* to cover the need of the sensitive (yet non-classified) personal computing of the 1% most targeted law-abiding citizens and elected officials - and their close personal and professional associates - such as those hundreds of thousands hacked and hackable by NSO Group and similar tools.

For participating EU states, TCCB and Seevik Net will allow them to **move ahead decisively and without hesitation** to (1) adequately protect the security, privacy, accountability and democratic nature of the sensitive communications and social interactions of their most sensitive officials, institutions and citizens; while at once (2) **leading by example** to positively influence the debate of newly proposed EU Regulations and Acts that are supposed to solve the same problem (e.g., EU Cyber Resilience Act, EU Media Freedom Act, EU Cybersecurity Act).

SPECIAL BENEFITS FOR SMALL NATIONS

The problem of hacking of their leaders and elected officials is especially dire for smaller countries like **Switzerland, Malta or Liechtenstein** - as well as inter-governmental organizations like the UN or ICRC - because they have **less capacity to control the entire supply chain to build classified mobile systems that they can trust**. So, they find themselves forced even more than others to discuss classified or top-secret matters using commercial smartphone devices, or classified phones reliant on obscure foreign technologies and suppliers.

At times, smaller states have more strategic autonomy and neutrality than larger ones to lead international impactful initiatives for the global public good and for peace, as shown by Liechtenstein led in the UN veto initiative, and Switzerland lead UN agreements for responsible cyber behavior. Plus, they often host significant financial centers that would benefit significantly from globally unique confidentiality offerings by their financial institutions, while also preventing its abuse to commit grave financial and other crimes.

SPECIAL CASE FOR THE US, ISRAEL AND CHINA

Initial participation by **dominant cyber states like the US, China and Israel** as founding governance partners of the TCCB and Seevik Net would be welcome but **not required**. Also, it would be incentivized via **higher temporary influence** for the ones that join earlier rather than later.

The US, China or Israel**,** while being the dominant western cyber powers, would counterintuitively overall greatly benefit from joining TCCB and Seevik.

The problem with the status quo

The current model by which western states reconcile the need for **sensitive non-classified mobile** privacy and security with the need for international *legitimate* lawful access is causing **increasingly unacceptable collateral damages in terms of civil freedoms and democratic sovereignty** in EU member states, of the EU, the world over, and just as much within the US and Israel, with even parliamentarians and the former prime ministers vulnerable. Even heads of state and head of opposition, and their close associates, were hacked on their smartphones last year, as shown in Spain, in Greece and in Israel, in Finland, in UK, in Switzerland, among those we got to know about.

The problem has long turned also in a crucial state **security threat,** even in the US and Israel, as it increasingly exposes our leaders, elected officials and journalists to spying and blackmail - by enemies foreign and domestic - and mines the appeal of our democracies to our fellow citizens and towards third states, whose "hearts and minds" we need to prevail over fast rising appeal authoritarian countries and of authoritarianism.

Why the US, China and Israel benefit the status quo

It may seem that the US and Israel, would not have an interested in maintaining the status quo in the market, because they **undoubtedly have an "informational superiority upper hand" in the current model**, via their overwhelming control of leading secure devices (e.g. iPhone, Android), spyware (e.g. NSO Group) and endpoint security firms (Crowdstrike, Koolspan, etc).

Due to their control over the leading and globally-hegemonic private IT security firms, the US and Israel have an apparent distinct advantage, via their ability to access better protections, better espionage capabilities, and better espionage countermeasures. **Similar powers over the security and insecurity of mobile infrastructure is exercised, increasingly, by China**, via its control of nearly all mobile phones except iPhones, and leadership in 5G networks, and increasingly with platforms like WeChat, TikTok and the new mobile operating system Harmony.

Why the US, China and Israel are greatly damaged by the status quo.

Yet, the current model and hegemony comes with **huge and mounting inefficiencies, collateral damages, and a “boomerang effect”** for those leading states, so it may be worth exploring it there may be a better alternative model, like ours, that would eliminate or radically mitigate those effects, and overall be **most convenient for such states and also for the narrower goals of their security agencies**.

Even though they have the upper hand in the current scenario, they are suffering from huge collateral damages mining their own democratic systems. Involuntarily, **they have ended up weakening the technologies, procedural safeguards and oversight processes of the IT systems that are most critical in sustaining democratic society**, such as (a) the mobile devices used by even their top elected officials, parliamentarians, ministers, as well as (b) the targeted hacking systems used to by the police.

This has become even more evident when even the son of the prime minister of Israel Netanyau was reportedly hacked, with no way to know if and by who he was, in a cascade of accusations, severe divisions in society, and further **loss of trust in democratic institutions**. It has become clear that **every elected official or citizen not only abroad but also in their country is hackable by who knows who,** inside or outside their institutions. In addition, sometimes they "go dark" and the evidence they acquire is often unreliable, and not accepted by their highest courts.

Even the president of the US runs very similar risks, as detailed in 2017 by the New York Times. Just as concerning, current smartphones enable users to reliably delete evidence of crimes to evade criminal accountability, as shown by investigations on the US president's secret service detail, while others may have acquired such evidence before its deletion for use in politically-motivated blackmail.

For these reasons, and more detailed below, we believe they will eventually join as governance partners of the TCCB, **even though they'll need approval from an UN-like neutral democratic body to intercept an elected official, journalist or private citizen from a friendly nation**. While nearly every state would be welcome to join such an initiative, none is necessary. That said, it would be highly advantageous that a few states that have a key role in current and future global cybersecurity architecture - like the US, Israel and/or China - would join sooner or later.

Traction with the US, China and Israel

Over the last two years, we held over nine meetings of intense and detailed dialogue with the former highest-ranking cyber diplomats of both the **US and Israel.** Following such dialogues, we wrote a blog post on why **Israel** and the **US** should and will eventually join as governance partners of the Trustless Computing Certification Body - even though they'd need approval by an UN-like resilient, democratic body to intercept an elected official or private citizen from a friendly nation. MACH37, the Virginia-based US leading cybersecurity accelerator, for which we were chosen among hundreds in Q4 2021, has accrued rights to 3% of the shares of the spin-in TRUSTLESS.AI.

We have engaged with some interest with several top executives of **Huawei** global and Swiss in 2019-2020, as one of two smartphone partners (one western and one non-western) for building initial mobile device and system complaint to the TCCB Seevik Phone, and as a proxy for engaging with the Chinese government. We made some attempts to engage China, over the years, without success. But last November, we initially engaged a **Secretary of the China Mission to the UN in Geneva**, in charge of IT standards at the UN.

Why should cyber superpowers ideally join TCCB together rather than singularly?

When and if the US and/Israel decide to participate, we believe it would be crucial to ensure that China also participated or that it would be ensured that it can join later, and the other way around. That's because it would make TCCB, Seevik Net and TCCB-compliant IT:(1) more equally trusted worldwide, to **enable the fair and effective global dialogue,** at all levels, to promote **peace and joint tackling of global challenges;** and (2) substantially **more trusted even by western citizens, elected officials, diplomats**, and even prime ministers, given the experience of programs like Crypto AG, NSO Group, the iPhone, and past overreach of western security agencies.

NEXT STEPS & ROADMAP

On **March 15-16th 2023,** we'll hold the 9th Edition of our Free and Safe in Cyberspace, in **Geneva** for the third time, with representatives of states, NGOs and IGOs, Swiss and Geneva authorities and NGOs and IGOs. that are potentially interested in joining TCCB and Seevik Net will meet in closed doors and/or public meetings. Main focus will be on *Ministries of Foreign Affairs* and *Missions to the UN in Geneva* of interested states.

By **April 2023**, we aim to have co-founder states on-boarded - via LoI or binding agreement or at least engaged in a "TCCB founding process" via closed-door and public meetings online and offline - that will revise the current TCCB statute/governance and the Trustless Computing Paradigms. After six months, TCCB will be **open to participation to all states on a fair and equal basis**. TCCB is bound by statute to strive to achieve a very high global representativity already as it reaches 20 member states, also via weighted voting.

By **Q1 2025**, we plan to become operational with TCCB issuing certifications and to ship initial TCCB-compliant mobile IT systems/services, including a batch of 15,000 mobile client device units reserved for our initial limited-exclusive partnering states, NGOs and IGOs, and a few select private entities.

JOIN US TO LEARN AND CO-DEVELOP THIS OPPORTUNITY

To learn more about this opportunity, we invite you to join us in closed-door meetings with other like-minded states, NGOs and IGOs for the *9th Edition of the Free and Safe in Cyberspace conference*, to be held in **Geneva next March 15-16th.**

Attendance to the meetings are possible with the **status of *Observer* or *Full Participant***. *Participant* states receive written guarantees that they have a reserved option to be part of no more than 3 EU and 4 non-EU states will be *Founding Partners* of TCCB, enjoying special limited-time benefits.

CONTACTS

Trustless Computing Association - www.trustlesscomputing.org —
Rufo Guerreschi, Exec. Director - rufo@trustlesscomputing.org
+41225483778 --- +393289376075
Geneva - Rome

MORE INFO & DOCUMENTS

- Executive Summary - Opportunity for States, IGOs and NGOs,(This Document!) a 20-page A4 PDF, preceded by a 2 pager Summary, detailing our offer to join as *cofounder partners*.
- Terms of Participation to FSC9 for the TCCB and Seevik Net initiative, a 4-pager that will guarantee your spot in the upcoming meetings, as *observer* or as a *full participant.* It is to be signed at least 7 days before each of the meetings. Spots for states are limited to seven, and accepted largely on a "first come, first serve" basis.
- Last January 31st, 2023, **an opinion article by our director Rufo Guerreschi was published on Le Temps, Geneva most-read daily newspaper** in a 900-words version for th paper edition and a longer 3000-words version with links on their digital version. In recent years, the same daily published two articles about us and one other opinion article, as you can see in our press section.
- Introduction Slide Deck, a 40-pager intro deck PDF on our association, partners, advisors, and vision.
- Here is a list of speakers to previous FSC editions.
- Available after qualified request, and a signed NDA or signed Terms of Participation agreement: a *Detailed Traction Update*, a 25-pager deck PDF profiling our current R&D and governance partners of TCA, TCCB and Seevik Net, as well as the extensive interest shown so far by several countries - through their relevant ministry, strategic IT security companies, and cyber-only funding vehicles - with a 2-pager summary on top.